

PIKOPLATNOŚCI STRUMIENIOWE W INTELIGENTNYCH MIASTACH

SYGN. WIB PAB 19/2020



Raport opracowany na zlecenie Programu Analityczno-Badawczego
Fundacji Warszawski Instytut Bankowości

Poznań, 2020

 PROGRAM
ANALITYCZNO
BADAWCZY

O Raporcie

Raport **Pikopłatności strumieniowe w inteligentnych miastach** został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości

Autorzy:

Raport przygotowany przez zespół w składzie:

dr Daniel Wilusz

dr hab. inż. Jarogniew Rykowski, prof. UEP

prof. dr hab. inż. Wojciech Cellary



O Programie

Program Analityczno-Badawczy przy Fundacji WIB powstał w 2019 roku jako odpowiedź na potrzeby sektora bankowego w zakresie analizy zjawisk, tworzenia opracowań i porządkowania wiedzy w obszarach cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego, kształtującego warunki działania banków w Polsce. Prace analityczno-badawcze w ramach programu realizowane są pod kątem możliwości praktycznego wykorzystania ich wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz kreowania wartości dla klientów bankowości. PAB WIB kładzie duży nacisk na rozwój współpracy ze środowiskami akademickimi i eksperckimi, poszukując synergii w zakresie zainteresowań badawczych autorów oraz potrzeb rozwojowych sektora bankowego.

W ramach programu realizowane są analizy i badania w następujących obszarach:

-  **Nowe technologie i cyberbezpieczeństwo**
-  **Zdolność banków do finansowania gospodarki**
-  **Bankowość spółdzielcza**
-  **Rynek nieruchomości**
-  **Zielony ład i finansowanie energetyki odnawialnej**
-  **Finansowanie projektów innowacyjnych**

Więcej na temat działalności programu na stronie www.pab.wib.org.pl

Kontakt:

dr Andrzej Banasiak
Koordynator Programu
m: 696 405 104
e: abanasiak@wib.org.pl

Jacek Gieorgica
m: 603 626 254
e: jgieorgica@wib.org.pl

Warszawski Instytut Bankowości
00-394 Warszawa, ul. Solec 38, lok 104
t: (22) 182 31 70
e: pab@wib.org.pl

Agnieszka Nierodka
m: 607 484 391
e: anierodka@wib.org.pl

dr Tomasz Pawlonka
m: 505 917 778
e: tpawlonka@wib.org.pl



Spis treści

	Streszczenie kierownicze	6
	ROZDZIAŁ I. Wstęp	10
	ROZDZIAŁ II Koncepcja systemu płatności strumieniowych AMFI	13
	ROZDZIAŁ III Charakterystyka płatnych usług świadczonych w przestrzeni miejskiej	17
	3.1. Zamiana usług bezpłatnych na płatne strumieniowo	18
	3.2. Charakterystyka płatności strumieniowych	18
	3.3. Klasyfikacja opłat za usługi w inteligentnym mieście	19
	3.4. Potencjał rozwoju płatnych usług automatycznych	20
	3.5. Zalety pikopłatności strumieniowych dla usługodawców	21
	3.6. Zalety pikopłatności strumieniowych dla usługobiorców	22
	3.7. Zalety pikopłatności strumieniowych dla banków	22
	3.8. Uzasadnienie potrzeby pikopłatności strumieniowych	22
	ROZDZIAŁ IV. Cechy systemu pikopłatności strumieniowych AMFI	23
	ROZDZIAŁ V. Architektura systemu pikopłatności w inteligentnym mieście	26
	ROZDZIAŁ VI. Techniczna realizacja systemu AMFI	30
	6.1. Założenia wstępne	31
	6.2. Pobór opłat i świadczenie usługi lokalnie	32
	6.3. Pobór opłat i świadczenie usługi zdalnie	33
	6.4. Modyfikacje rozgłaszania identyfikatora	33
	6.5. Kwestie implementacyjne	34
	ROZDZIAŁ VII. Protokoły systemu AMFI	35
	7.1. Protokół wydawania rulonu pikomonet	36
	7.2. Protokół inicjowania płatności strumieniowej	37
	7.3. Protokół strumieniowych pikopłatności	38
	7.4. Protokół wykupu pikomonet	39
	7.5. Proponowany interfejs programowy dla celów komunikacji płatników z bankiem rozliczającym pikomonety	41
	7.6. Proponowany interfejs programowy protokołu systemu pikopłatności w inteligentnym mieście na styku płatnik – usługodawca	41
	7.7. Proponowany interfejs programowy protokołu systemu pikopłatności w inteligentnym mieście na styku usługodawca – bank	42



VIII	ROZDZIAŁ VIII. System pikopłatności strumieniowych w świetle Ustawy o usługach płatniczych oraz rozporządzenia Komisji Europejskiej 2018/389	43
	8.1. Konstrukcja systemu AMFI w kontekście definicji prawnych	44
	8.2. Silne uwierzytelnianie	44
	8.3. Możliwość odstępstwa od niektórych regulacji prawnych w przypadku mikropłatności	46
	8.4. Wyłączenie stosowania Ustawy o usługach płatniczych	47
	8.5. Wymagania odnośnie do zmiany obowiązujących przepisów	48
	8.6. Podsumowanie	48
IX	ROZDZIAŁ IX. Analiza kosztów wdrożenia systemu AMFI	49
	9.1. Koszty związane z przygotowaniem demonstratora technologii	50
	9.2. Koszty związane z utrzymaniem systemu AMFI po stronie banku	51
	9.3. Koszty po stronie odbiorców płatności (usługodawców)	52
X	ROZDZIAŁ X. Możliwości wdrożenia systemu AMFI w inteligentnych miastach	53
XI	ROZDZIAŁ XI. Propozycja dalszych badań	57
	Bibliografia	59



Streszczenie kierownicze

W ostatnim czasie obserwujemy niezwykle dynamiczny rozwój inteligentnych miast spowodowany wdrażaniem w nich rozwiązań opartych na nowych technologiach informatyczno-komunikacyjnych. Mają one na celu obniżenie kosztów, poprawę bezpieczeństwa, zmniejszenie obciążenia środowiskowego i zmniejszenie zużycia energii, prowadząc jednocześnie do podniesienia jakości życia mieszkańców miast. Zmiany technologiczne umożliwiają wprowadzanie innowacyjnych modeli biznesowych, wśród których ważny jest model płatności za usługi proporcjonalnie do ich użycia. Umożliwia on racjonalizację użycia zasobów, których koszty ponoszą ci, którzy z nich korzystają – zarówno mieszkańcy, jak i przyjezdni – a nie tylko płatnicy lokalnych podatków. Ten model wymaga jednak nowej metody płatności, która z jednej strony byłaby skuteczna, wygodna i uniwersalna, a z drugiej – zapewniała płatnikom prywatność. Taka metoda jest opisana w tym raporcie – realizuje ją system pikopłatności strumieniowych AMFI.

W systemie AMFI płatność nie jest jednorazowym aktem, tak jak to ma miejsce w przypadku płatności gotówką, kartą płatniczą lub Blikiem, tylko ma postać strumienia pikomonet o ustalonej wartości, które są przekazywane ze smartfonu płatnika do odbiorcy płatności tak długo, jak długo jest płatnikowi świadczona pewna usługa. Taka płatność może być inicjowana i kończona automatycznie, o ile płatnik zadeklaruje, że ma zaufanie do konkretnego usługodawcy.

Podstawą systemu AMFI są dedykowane protokoły płatności pieniądzem elektronicznym (pikomonetami), oparte na algorytmach kryptograficznych. Protokoły te zapewniają z jednej strony bezpieczne przekazywanie pikomonet z aplikacji zainstalowanej na smartfonie płatnika do odbiorcy płatności bezprzewodową drogą elektroniczną, a z drugiej pozwalają płatnikowi zachować anonimowość – odbiorca płatności wie, ile otrzymał pikomonet, ale nie wie, od kogo je otrzymał.

W systemie AMFI szczególną rolę odgrywają banki: bank płatnika, który jest wydawcą pieniądza elektronicznego w formie rulonu pikomonet, oraz bank odbiorcy płatności, który rozlicza otrzymane pikomoney. Jeden bank może pełnić obie te role.

Płatności strumieniowe służą przede wszystkim do opłat za usługi trwające przez pewien czas, za które usługobiorca automatycznie płaci proporcjonalnie do tego czasu. Oznacza to płatność za przebywanie w pewnym miejscu – na przykład w muzeum, na placu zabaw, na parkingu, na pływalni, w autobusie lub w tramwaju itp. lub za korzystanie z pewnego urządzenia – np. roweru miejskiego, hulajnogi, ładowarki samochodu elektrycznego itp. Płatności strumieniowe zrównoleglają świadczenie usługi w czasie z płatnościami w czasie, co umożliwia automatyzację płatności.

Proponowany system pikopłatności jest oryginalny w skali światowej. Autorom raportu nie są znane żadne przykłady stosowania systemu podobnego w założeniach do proponowanych pikopłatności w żadnym kraju na świecie, włączając w to wiodące technologicznie państwa: Japonię, Koreę Południową, Stany Zjednoczone oraz zachodnią Europę. Według najlepszej wiedzy autorów nie ma aktualnie publikacji naukowych na ten temat. Publikacje naukowe ze zbliżonego zakresu odnoszą się co najwyżej do szczególnych technik kryptograficznych, wykorzystywanych w innych formach pieniądza elektronicznego.

W raporcie przedstawiono i omówiono 11 cech systemu pikopłatności strumieniowych AMFI:

- Cecha 1: Zapewnienie ostatecznego rozliczenia transakcji
- Cecha 2: Zapewnienie bezpieczeństwa obrotu środkami płatniczymi
- Cecha 3: Obsługa strumienia pikopłatności
- Cecha 4: Umożliwienie płatności sporadycznych
- Cecha 5: Odporność na zerwanie komunikacji
- Cecha 6: Zapewnienie anonimowości płatnika
- Cecha 7: Odporność na fałszerstwo pieniądza elektronicznego
- Cecha 8: Odporność na nieuprawnione wielokrotne użycie pieniądza elektronicznego



- Cecha 9: Uniwersalność
- Cecha 10: Skalowalność
- Cecha 11: Automatyzm

W raporcie przedstawiono architekturę systemu AMFI z uwzględnieniem jego przeznaczenia, neutralności ekonomicznej, wielości uczestników systemu, anonimowości płatnika, przejrzystości banku i odbiorcy płatności, zapobiegania oszustwom, urządzeń płatników, niskich kosztów strumienia pikopłatności, wymagań niefunkcjonalnych i komponentów. Przedstawiono techniczne aspekty systemu AMFI oraz jego protokoły, uzupełnione o opis interakcji między płatnikiem, odbiorcą płatności i bankiem:

- 1) protokół wydawania rulonu pikomonet;
- 2) protokół inicjowania płatności strumieniowej;
- 3) protokół strumieniowych pikopłatności;
- 4) protokół wykupu pikomonet.

Zaproponowano również interfejsy programowe dla celów komunikacji.

W raporcie szczegółowo przeanalizowano system pikopłatności strumieniowych AMFI w świetle Ustawy o usługach płatniczych oraz rozporządzenia Komisji Europejskiej 2018/389. Z analizy wynika, że

wdrożenie systemu AMFI jest w obecnej sytuacji prawnej możliwe w ograniczonym stopniu, jako systemu płatności za usługi oferowane przez jednostki sektora finansów publicznych, w tym miasta. W celu upowszechnienia zastosowania systemu AMFI jako usługi płatniczej, konieczne jest wprowadzenie określonych zmian prawnych, regulujących automatyczne mikropłatności z użyciem pieniądza elektronicznego, które to zmiany zaproponowano w tym raporcie.

Następnie przedstawiono kategorie kosztów, z którymi należy się liczyć przy wdrażaniu systemu AMFI, w podziale na koszty jednorazowe, związane z przygotowaniem demonstratora technologii, koszty związane z utrzymaniem systemu AMFI po stronie banku oraz koszty po stronie odbiorców płatności (usługodawców).

W kolejnym rozdziale raportu przedstawiono szereg możliwych zastosowań systemu AMFI w inteligentnym mieście. Należy jednak podkreślić, że konkretne zastosowania wymagają przygotowania odrębnych, szczegółowych studiów wykonalności, których celem byłaby analiza możliwości połączenia danej usługi z systemem pikopłatności strumieniowych AMFI.

W ostatnim rozdziale przedstawiono kierunki dalszego rozwoju prac nad zaproponowanym systemem anonimowych pikopłatności strumieniowych AMFI, których wynikiem byłby demonstrator technologii systemu AMFI, funkcjonujący w warunkach zbliżonych do rzeczywistych.

0 autorach

Dr Daniel Wilusz jest informatykiem i ekonomistą, od 2010 roku związanym naukowo i zawodowo z Katedrą Technologii Informatycznych na Uniwersytecie Ekonomicznym w Poznaniu, specjalizującym się w biznesowych zastosowaniach protokołów kryptograficznych, systemach elektronicznych płatności oraz Internecie Rzeczy. W 2010 roku ukończył z wyróżnieniem specjalność elektroniczny biznes na Wydziale Zarządzania Uniwersytetu Ekonomicznego w Poznaniu, a w 2019 roku obronił rozprawę doktorską w dyscyplinie informatyka techniczna i telekomunikacja na Wydziale Informatyki i Zarządzania Politechniki Wrocławskiej. Jest autorem ponad 20 publikacji naukowych, w tym jednej w czasopiśmie z tzw. Listy Filadelfijskiej, za współautorstwo której otrzymał nagrodę zespołową Rektora Uniwersytetu Ekonomicznego w Poznaniu. Był wykonawcą w trzech międzynarodowych projektach, które dotyczyły Internetu Rzeczy (program POLLUX Narodowego Centrum Badań i Rozwoju – Luksemburg), bezpieczeństwa przetwarzania danych (USA) oraz kryptowalut (Japonia). W ramach pracy dydaktycznej prowadzi zajęcia z takich przedmiotów, jak zarządzanie projektami, strategię elektronicznego biznesu, programowanie komputerów, bazy danych oraz Internet Rzeczy. W 2015 roku w ramach projektu systemowego TransFormation.doc Ministerstwa Nauki i Szkolnictwa Wyższego uczestniczył w trzytygodniowym kursie szkoleniowym „Train the trainer course” zrealizowanym w Ivey Business School Western University w Kanadzie.

Dr hab. inż. Jarogniew Rykowski, profesor Uniwersytetu Ekonomicznego w Poznaniu, od roku 1986 do 1992 pracował w Instytucie Informatyki Politechniki Poznańskiej. Uczestniczył w tym czasie w kilku projektach badawczych, w tym w dwóch projektach rządowych (wspólnie z ZE ELWRO we Wrocławiu): 8.10 i 8.33, mających na celu opracowanie i wdrożenie do produkcji seryjnej sprzętu i oprogramowania profesjonalnych systemów wielomikrokomputerowych i mikrokomputera szkolnego. W ramach tego ostatniego projektu był jednym z głównych projektantów sieci komputerowej Junet i kompilatora języka LOGO, które później zostały także zaimplementowane na komputerze IBM PC (w ramach zamówienia Ministerstwa Edukacji Narodowej). Od roku 1992 do roku 1996 pracował, początkowo jako asystent, a następnie

adiunkt, we Francusko-Polskiej Wyższej Szkole Nowych Technik Informatyczno-Komunikacyjnych (EFP). Po zlikwidowaniu tej uczelni przeszedł do Akademii Ekonomicznej w Poznaniu, gdzie współuczestniczył w tworzeniu Katedry Technologii Informatycznych. Od roku 1996 do chwili obecnej jest pracownikiem tej Katedry, od lipca 2010 r. na etacie profesora UEP. W latach 2015-2017 był koordynatorem polsko-luksemburskiego projektu POLLUX-GOLIATH, który miał na celu opracowanie narzędzi i procedur sterowania e-komfortem za pomocą urządzeń Internetu Rzeczy, obecnie współpracuje z firmą Amica S.A. na polu projektu nowej klasy interfejsów dla urządzeń kuchennych przy wykorzystaniu sieci Bluetooth Mesh.

W czasie swojej pracy odbył szereg staży zagranicznych, spędzając m. in. dwa miesiące na Uniwersytecie w Eindhoven, szereg tygodni na Uniwersytecie Paris-Dauphine, dwa tygodnie na Uniwersytecie w Stuttgarcie oraz kilka miesięcy w ośrodkach naukowo-badawczych firmy Bull (Francja). Został dwukrotnie wyróżniony nagrodami Ministra Edukacji Narodowej, zespołowymi I i II stopnia oraz kilkakrotnie nagrodami Rektorów Politechniki Poznańskiej i EFP. Jest koordynatorem międzyuczelnianego kierunku studiów Aplikacje Internetu Rzeczy (wspólnie z Wydziałem Fizyki UAM w Poznaniu). Jest laureatem nagrody specjalnej przyznanej przez Kapitułę XIII Kongresu Gospodarki Elektronicznej i Związek Banków Polskich za utworzenie i prowadzenie tego innowacyjnego kierunku studiów. Jest autorem i współautorem trzech książek, około 70 artykułów naukowych opublikowanych w materiałach konferencyjnych i czasopismach (krajowych i zagranicznych) oraz dwóch patentów i sześciu wniosków patentowych.

Prof. dr hab. inż. Wojciech Cellary jest informatykiem, kierownikiem Katedry Technologii Informatycznych na Uniwersytecie Ekonomicznym w Poznaniu, specjalizującym się aktualnie w problematyce elektronicznego biznesu, elektronicznej gospodarki opartej na wiedzy, elektronicznej administracji, społeczeństwa informacyjnego, inteligentnych miast i multimediów. Pracował na dziewięciu uczelniach, trzech w kraju i sześciu za granicą we Francji i Włoszech. Ponadto był profesorem wizytującym w Macao S.A.R. Chiny i w Portugalii. Jest autorem 10 książek i ponad 180



artykułów naukowych. Był konsultantem wielu ministerstw, komisji sejmowych i senackich oraz ekspertem Komisji Europejskiej. Był głównym organizatorem ponad 50 naukowych konferencji krajowych i międzynarodowych, a ponadto członkiem komitetów programowych ponad 330 konferencji. Kierował licznymi projektami naukowymi i przemysłowymi, krajowymi i międzynarodowymi, finansowanymi przez przemysł polski, francuski i amerykański, polskie ministerstwa oraz Komisję Europejską. Jest członkiem licznych towarzystw i organizacji naukowych. W latach 2010-2011 pełnił funkcję przewodniczącego

Rady Informatyzacji przy Ministrze Spraw Wewnętrznych i Administracji, w latach 2012-2013 był członkiem Rady Informatyzacji przy Ministrze Administracji i Cyfryzacji, od 2002 roku jest członkiem Rady ds. Informatyzacji Edukacji przy Ministrze Edukacji Narodowej (dawniej Rady ds. Edukacji Informatycznej i Medialnej). Na jego wykłady uczęszcza około 700 studentów rocznie. Wśród przyznanych mu licznych nagród jest też laureatem nagrody „Ambasador Gospodarki Elektronicznej 2011” przyznanej przez Kapitułę VII Kongresu Gospodarki Elektronicznej i Związek Banków Polskich.



Wstęp



W ostatnim czasie obserwujemy niezwykle dynamiczny rozwój inteligentnych miast [PwC 2019]. Inteligencja tych miast objawia się efektywnym współdziałaniem szeregu instytucji, jednostek administracji, przedsiębiorstw, organizacji pozarządowych i obywateli [Deloitte 2018, ISO 2015]. Ma to na celu nie tylko polepszenie poziomu życia, ale także zmniejszenie kosztów i czasu realizacji procesów, zwiększenie ich zasięgu itp. Współdziałanie podmiotów w przestrzeni miejskiej jest istotne głównie ze względu na rosnący poziom urbanizacji, koncentracji miejsc zamieszkania i pracy, coraz większe potrzeby w zakresie wypoczynku i szeroko rozumianej rekreacji oraz rozrywki, zróżnicowanie społeczne (w tym problemy ludzi starszych, niepełnosprawnych i wykluczonych) [Sujata i inni 2016].

Administracja miasta i jednostki gospodarcze, działające na jego terenie, świadczą określone usługi na rzecz mieszkańców. Duża część tych usług jest lub w najbliższej przyszłości stanie się płatna. W celu zapewnienia zrównoważonego rozwoju, środowisko inteligentnego miasta wymaga rynku, który pozwala na coraz większy poziom automatyzacji przy świadczeniu takich usług oraz udostępniania zasobów miejskich, zestawiając oczekiwania konsumentów z technicznymi możliwościami dostawców przy jednoczesnym zapewnieniu niskich kosztów transakcyjnych [ISO 2015]. Postęp technologiczny pozwala na zwiększenie liczby i zakresu usług, nie tylko tych świadczonych bezpośrednio przez jednostki organizacyjne i podległe miastu, ale także realizowanych przy zaangażowaniu podmiotów prywatnych w realizację usług w przestrzeni miejskiej na zasadach partnerstwa publiczno-prywatnego [Woetzel i Remes 2018].

Postępująca cyfryzacja naturalnie wymusza zmiany w sposobie świadczenia usług. Z perspektywy odpłatnych usług świadczonych w inteligentnych miastach największy wpływ mają [Deloitte 2015b]:

- 1) zastąpienie posiadania przez wynajem – informatyzacja pozwala na elastyczne współdzielenie zasobów, co jest szczególnie korzystne dla podmiotów korzystających z tych zasobów sporadycznie. W przypadku niektórych zasobów, ich wykorzystanie przez właścicieli jest niskie, a czas, podczas którego są one niewykorzystane, powoduje marnotrawstwo potencjalnych przychodów oraz powoduje, że koszty stałe ich posiadania obejmują znaczną część kosztów całkowitych [WEF 2018]. Można tego uniknąć zastępując posiadanie przez wynajem. Przykładem jest zastąpienie posiadania samochodu na własność przez wynajem samochodu na minuty, które oferuje użytkownikowi korzyść w postaci swobody przemieszczania się,
- natomiast zdejmując z niego liczne obowiązki ciążące na posiadaczu pojazdu. Wynajem pociąga za sobą opłaty zależne od czasu i wymaga dostosowywania obecnych form płatności do szybko zmieniającego się rynku, a także rosnących wymagań klientów co do wygody i dostępności płatności;
- 2) powszechna cyfryzacja i automatyzacja – elektroniczne kanały komunikacji zaczynają być powszechnie uwzględniane w łańcuchu wartości dla usług i produktów, co pociąga za sobą postulaty cyfryzacji i automatyzacji płatności za te usługi;
- 3) zaufanie i reputacja – w cyfrowej gospodarce technologia informatyczna jest wykorzystywana do budowania zaufania między usługodawcą a użytkownikiem, którzy niekoniecznie znają się wzajemnie [Sturm 2018]. Jest to szczególnie ważne w przypadku dokonywania płatności, zwłaszcza przy wykorzystaniu zaufanej strony trzeciej typu bank;
- 4) usługi świadczone na żądanie – w cyfrowej gospodarce klienci oczekują elastyczności ze strony usługodawców w zakresie czasu dostępności oraz miejsca świadczenia usług. To wymaganie dotyczy także sposobu płatności za skorzystanie z usługi;
- 5) eliminacja pośredników – w łańcuchach wartości jest preferowana strategia bezpośredniego dotarcia do klienta, co prowadzi do eliminacji pośredników, w tym pośredników w realizacji płatności;
- 6) koncentracja dostawców infrastruktury – podmioty oferujące infrastrukturę i pomoc dla usługodawców wykazują tendencję do koncentracji, która pozwala wykorzystać efekt ekonomii skali. Efekt ten dotyczy także dokonywania płatności i powszechnego trendu do unifikacji sposobu zapłaty za usługi z punktu widzenia klienta;
- 7) dopuszczanie do pobierania opłat za usługę wielu odbiorców płatności – jako przykład można podać Londyn. Opłaty za korzystanie z komunikacji miejskiej w tym mieście obsługuje ponad dziesięciu usługodawców, od banków i klasycznych kart płatniczych po Apple i Google Pay [TFL 2020a]. Dobrym przykładem podobnego rozwiązania tego problemu są też większe miasta w Polsce, na przykład Warszawa, Trójmiasto i Poznań [ZTM 2020]. Jednak z punktu widzenia miasta nie jest to optymalne rozwiązanie, ze względu na konieczność podpisywania wielu umów z poszczególnymi odbiorcami płatności i konieczność implementacji wielu protokołów płatniczych w kasach biletowych;



- 8) rozproszenie wśród dostawców niszowych usług – ze względu na konieczność specjalizacji, niektórzy usługodawcy koncentrują się wyłącznie na wąskiej grupie docelowej, jednak wszystkie te podmioty łącznie są w stanie odpowiedzieć na szerokie spektrum potrzeb klientów. Takie wyspecjalizowane usługi mogą być obsługiwane przez jeden zunifikowany sposób płatności, co zdecydowanie zwiększy ich atrakcyjność i wygodę z punktu widzenia ich klientów;
- 9) popularność modelu biznesowego opierającego się na płatnościach za użycie – użytkownicy płacą za każdą wykorzystaną jednostkę usługi [WEF 2018]; w chwili obecnej zapłata jest realizowana łącznie i obejmuje całą jednorazową interakcję z usługą – *niezależne rozliczenie finansowe każdej jednostki* z osobna umożliwiłoby opłaty proporcjonalne do stopnia wykorzystania usługi, ale naliczane w czasie niemal rzeczywistym, a nie opłacane w całości z góry lub z dołu.



Koncepcja systemu płatności strumieniowych AMFI



W tym rozdziale jest opisana koncepcja systemu anonimowych pikopłatności strumieniowych AMFI za usługi świadczone w inteligentnych miastach. W celu zapewnienia wspólnej bazy pojęciowej, poniżej zdefiniowano najważniejsze pojęcia wykorzystane do opisu systemu.

płatnik – osoba fizyczna, osoba prawna lub jednostka organizacyjna niebędąca osobą prawną, składająca zlecenie płatnicze. W tym opracowaniu płatnikiem jest usługobiorca.

odbiorca płatności – osoba fizyczna, osoba prawna lub jednostka organizacyjna niebędąca osobą prawną, będąca odbiorcą środków pieniężnych. W tym opracowaniu odbiorcą płatności jest usługodawca.

pieniądz elektroniczny – wartość pieniężna przechowywana elektronicznie, w tym magnetycznie, wydawana, z obowiązkiem jej wykupu, w celu dokonywania transakcji płatniczych, akceptowana przez podmioty inne niż wyłącznie wydawca pieniądza elektronicznego [Ustawa 2020/794].

pikopłatność – płatność, której wartość może być niższa niż najmniejsza jednostka w danej walucie, np. ułamek grosza.

strumień pikopłatności – seria następujących po sobie pikopłatności, w której wcześniejsza poprawna płatność pozwala na automatyczne zweryfikowanie poprawności kolejnej płatności.

system pikopłatności – system informatyczny pozwalający bankom na wydawanie pieniądza elektronicznego, płatnikom na składanie zleceń płatniczych przy wykorzystaniu pieniądza elektronicznego, a odbiorcom na odbieranie środków pieniężnych przy wykorzystaniu pieniądza elektronicznego.

pikomoneta – pieniądz elektroniczny, którego nominał może być mniejszy od najmniejszej jednostki pieniężnej przewidzianej dla waluty, w której jest denominowany.

rulon pikomonet – zestaw powiązanych ze sobą pikomonet, które mogą być wydatkowane strumieniowo, w kolejności w jakiej wchodzi w skład rulonu pikomonet.

zestaw reguł płatności – dane określające jednostkę świadczonej usługi, cenę za jednostkę tej usługi, minimalną liczbę jednostek usługi, które trzeba nabyć oraz maksymalny czas blokady rulonu pikomonet na rzecz odbiorcy płatności (usługodawcy).

W raporcie przedstawiono anonimowe pikopłatności strumieniowe, które są formą pieniądza elektronicznego, umożliwiające dokonywanie licznych, automatycznych, niskokwotowych (nawet ułamki grosza) i wysokokwotowych płatności w trakcie korzystania z usług świadczonych przez dowolnych usługodawców w przestrzeni miejskiej. Zamiast płatności rozumianej jako pojedynczy akt realizowany bezpośrednio przez płatnika za pomocą gotówki, karty lub smartfonu, zaproponowano strumień elektronicznych pikomonet, przelewanych okresowo ze smartfonu płatnika tak długo, jak długo korzysta on z określonej usługi.

Podstawą proponowanego rozwiązania są dedykowane protokoły płatności pieniądzem elektronicznym oparte na algorytmach kryptograficznych. Protokoły te zapewniają z jednej strony możliwość realizacji pojedynczych płatności na bardzo małe kwoty, a z drugiej strony, dzięki zastosowaniu kryptograficznego protokołu ślepych podpisów, uniemożliwiają powiązanie przez usługodawcę (odbiorcę płatności) tych płatności z tożsamością usługobiorcy (płatnika).

Ogólną architekturę systemu anonimowych pikopłatności strumieniowych AMFI przedstawia Rysunek 1. W systemie AMFI wyróżniamy czterech aktorów:

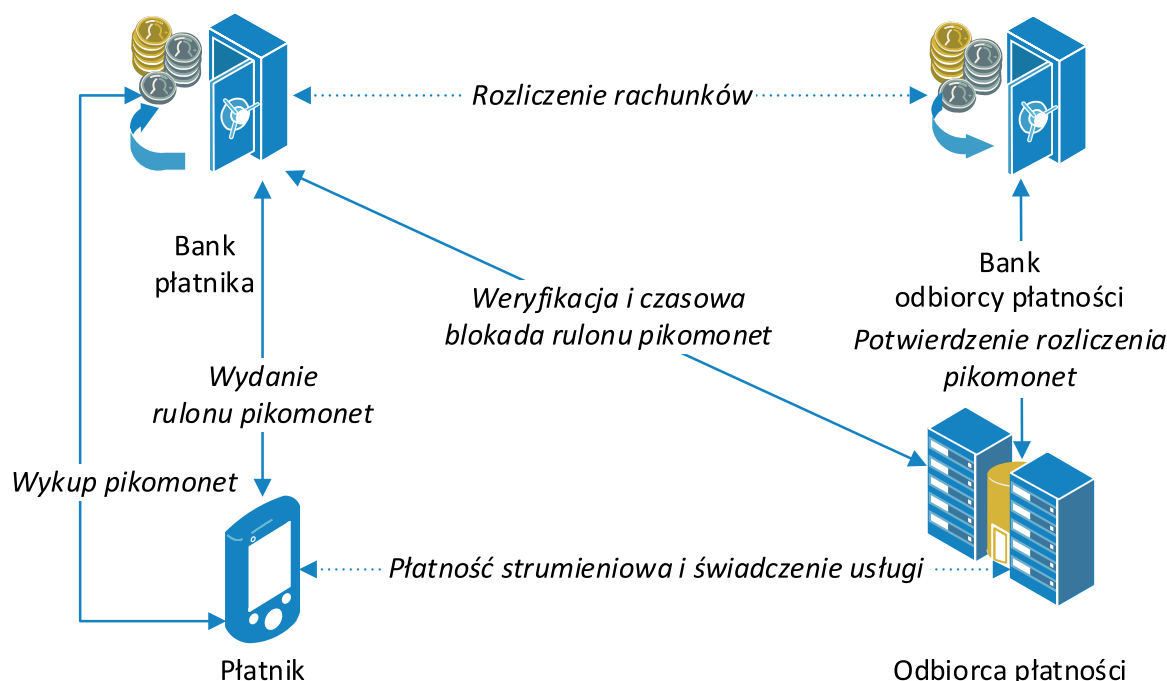
- 1) płatnika (usługobiorcę),
- 2) odbiorcę płatności (usługodawcę),
- 3) bank płatnika (wydawcę pieniądza elektronicznego),
- 4) bank odbiorcy płatności.

W szczególnym przypadku bank płatnika i bank odbiorcy płatności mogą być tym samym podmiotem.

Funkcje systemu AMFI są realizowane za pomocą czterech protokołów:

- 1) *Wydawania rulonu pikomonet;*
- 2) *Inicjacji płatności strumieniowej;*
- 3) *Strumieniowych pikopłatności;*
- 4) *Wykupu pikomonet.*

Płatnik, aby móc korzystać z systemu AMFI, zawiera z bankiem płatnika umowę o wydanie pieniądza elektronicznego, na skutek której zostaje mu udostępniona aplikacja, pozwalająca na uzyskanie pieniądza elektronicznego oraz dokonywanie anonimowych pikopłatności strumieniowych. Aplikacja ta, po zainstalowaniu na smartfonie płatnika, będzie pełnić rolę



Rysunek 1. Ogólna architektura systemu anonimowych pikopłatności strumieniowych AMFI

instrumentu płatniczego. W celu nabycia pieniądza elektronicznego płatnik, korzystając z instrumentu płatniczego, komunikuje się za pośrednictwem internetu z bankiem płatnika i rozpoczyna realizację protokołu wydawania rulonu pikomonet. Płatnik z odpowiednim wyprzedzeniem przekazuje do banku środki pieniężne, za pomocą przelewu lub obciążenia karty płatniczej, za które nastąpi wydanie anonimowego pieniądza elektronicznego (rulonu pikomonet). Po otrzymaniu środków pieniężnych, bank wydaje pieniądz elektroniczny, który jest zapisywany w instrumencie płatniczym.

Odbiorca płatności, aby móc uczestniczyć w systemie, musi zawrzeć z bankiem odbiorcy płatności umowę o akceptowaniu i obsłudze płatności realizowanych w systemie AMFI. W efekcie zawarcia umowy, bank odbiorcy udostępnia odbiorcy płatności aplikację pozwalającą na przyjmowanie anonimowych pikopłatności strumieniowych.

Dokonanie płatności przez płatnika wymaga od jego aplikacji wykonania protokołu inicjacji płatności strumieniowej u odbiorcy płatności. W tym celu aplikacja płatnika komunikuje się z aplikacją odbiorcy płatności i przekazuje dane konieczne do zainicjowania płatności w banku płatnika. Następnie aplikacja odbiorcy płatności weryfikuje prawidłowość otrzymanych danych i nawiązuje połączenie z bankiem płatnika, w celu ustanowienia czasowej blokady rulonu pikomonet, aby uniemożliwić płatnikowi wielokrotne posłużenie się tymi samymi pikomonetami.

Następnie aplikacja płatnika rozpoczyna protokół przetwarzania płatności, który pozwala na uiszczenie strumieniowych pikopłatności na rzecz odbiorcy płatności. Protokół ten polega na przekazywaniu przez aplikację płatnika za pomocą instrumentu płatniczego pikomonet do urządzenia odbiorcy płatności. Aplikacja odbiorcy płatności weryfikuje prawidłowość każdej otrzymanej pikomonet na podstawie poprzedniej, co zapewnia późniejsze rozliczenie wszystkich otrzymanych pikomonet przez bank odbiorcy.

Po zakończeniu realizacji strumienia pikopłatności przez aplikację płatnika, aplikacja odbiorcy płatności, przed upływem czasu blokady rulonu pikomonet, realizuje wspólnie z bankiem płatnika protokół rozliczenia pieniądza elektronicznego. Aplikacja odbiorcy płatności przekazuje bankowi płatnika między innymi ostatnią otrzymaną od płatnika pikomonetę, co pozwala bankowi odbiorcy na rozliczenie całego strumienia pikopłatności. W efekcie rozliczenia strumienia pikopłatności, bank płatnika uznaje rachunek odbiorcy płatności prowadzony przez bank odbiorcy oraz odblokowuje pikomonet niewykorzystane przez płatnika. Odbiorca płatności w dowolnym czasie może sprawdzić, czy bank płatnika uznał jego rachunek, korzystając z usług swojego banku.

Płatnik, aby dokonać wykupu niewykorzystanych jednostek pieniądza elektronicznego, realizuje protokół wykupu pikomonet. Protokół ten polega na dokonaniu przez płatnika płatności na własną



rzecz, zatem płatnik występuje jednocześnie w roli odbiorcy płatności. Za pomocą protokołu strumieniowych pikopłatności aplikacja płatnika przekazuje pikomonety, które chce umorzyć, do banku płatnika. Po przekazaniu jednostek pieniądza elektronicznego do banku płatnika, płatnik oczekuje na uznanie swojego konta.

Dzięki wykorzystaniu kryptograficznego protokołu ślepych podpisów i wymianie wyłącznie danych koniecznych do dokonania płatności, system AMFI chroni tożsamość płatnika, zapewniając jego anonimowość. Każdy z aktorów dysponuje tylko częściową wiedzą na temat przepływu pikomonet, niezbędną do realizacji swojej roli. Usługodawca (odbiorca płatności) wie, ile środków sumarycznie otrzymał z tytułu

świadczenia usługi, ale nie wie, ilu było płatników i kim oni byli. Bank odbiorcy wie, ile sumarycznie były warte usługi, za które zapłacił płatnik, i potrafi uznać rachunek usługodawcy, ale nie może jednoznacznie powiązać tożsamości płatników z usługami i usługodawcami. Płatnik wie, ile go kosztowała dana usługa, ale nie ma informacji o innych płatnikach i usługach, nawet tych realizowanych w tym samym miejscu i czasie, co usługa świadczona dla niego.

W systemie AMFI wyeliminowano obecność pośredników oraz konieczność rejestracji u usługodawców. Płatnik może też skorzystać z usługi jednorazowo, bez konieczności dokonywania przedpłaty lub rejestracji w systemie usługodawcy, gdyż system AMFI pozwala na bieżąco dokonywać płatności.



Charakterystyka płatnych usług świadczonych w przestrzeni miejskiej



3.1. Zamiana usług bezpłatnych na płatne strumieniowo

Usługi świadczone w przestrzeni miejskiej obywatelom dzielą się na płatne i bezpłatne. Koszty usług bezpłatnych są pokrywane z lokalnych podatków. Wiąże się z nimi istotny problem finansowy, gdyż korzystają z nich nie tylko płatnicy lokalnych podatków, ale także przyjezdni – turyści, studenci i mieszkańcy okolicznych gmin, którzy zwiedzają, studiują lub pracują w mieście i korzystają z jego usług, ale lokalne podatki odprowadzają w miejscu swojego zamieszkania. Wprowadzenie pikopłatności proporcjonalnych do użycia pozwoliłoby osobom przyjezdnym partycypować w opłatach na zasadach podobnych do tych, które obowiązują na autostradach – płacą tylko ci, którzy z danej autostrady korzystają i to proporcjonalnie do pokonanego dystansu. Jednak taki system opłat – proporcjonalnych do użycia danej usługi – musi być przyjazny dla użytkownika. Najlepiej, jeśli opłaty są pobierane automatycznie bez konieczności wykonywania specjalnych czynności osobiście przez użytkownika. Na autostradach taki poziom wygody zapewniają systemy elektronicznego poboru opłat – kierowca co najwyżej musi zwolnić przejeżdżając przez punkt poboru opłat, ale nie wykonuje żadnych dodatkowych czynności w celu wniesienia opłaty.

Wzrastająca liczba usług może też spowodować efekt nadmiaru i przesytu (ang. information overload), a w efekcie odwracanie się od nich obywateli. Efekt ten można zminimalizować unifikując płatności, jako czynności wspólnej dla wszystkich płatnych usług, najlepiej przez znany bank, jako jednostkę, która cieszy się zaufaniem społecznym [Deloitte 2015a]. Wprowadzenie jednolitego systemu pikopłatności strumieniowych, które są automatyczne, proporcjonalne do użycia i obejmują możliwie wszystkie usługi płatne w inteligentnym mieście spowoduje, że obywatele (płatnicy) szybko się do niego przyzwyczają, co znacznie zwiększy efektywność sposobu regulacji opłat za usługi. Niniejsze opracowanie pokazuje, że opracowanie takiego rozwiązania jest nie tylko możliwe, ale także efektywne i nieuciążliwe dla obu stron – zarówno płatnika, jak i odbiorcy płatności.

3.2. Charakterystyka płatności strumieniowych

Płatności strumieniowe służą przede wszystkim do wnoszenia opłat za usługi trwające przez pewien czas, za które usługobiorca automatycznie płaci proporcjonalnie do tego czasu. Oznacza to płatność za przebywanie w pewnym miejscu – na przykład w muzeum, na placu zabaw, na parkingu, na pływalni, w autobusie lub w tramwaju itp., lub za korzystanie

z pewnego urządzenia – np. roweru miejskiego, hulaj-nogi, ładowarki samochodu elektrycznego itp. Płatności strumieniowe zrównoleglają świadczenie usługi w czasie z płatnościami w czasie, co umożliwia automatyzację płatności.

Aktualnie rosnąca automatyzacja usług wymusza nowe, zautomatyzowane sposoby płatności [Deloitte 2015b]. Obecnie płatności (niestrumieniowe) wymagają każdorazowego zaangażowania płatnika albo w przekazanie gotówki, albo w przesunięcie kartą płatniczą nad czytnikiem, albo w potwierdzenie transakcji w aplikacji zainstalowanej i uruchomionej w smartfonie lub za pomocą systemu BLIK. Zautomatyzowane płatności wykluczają każdorazowe zaangażowanie płatnika, które jest wręcz zaprzeczeniem automatyzacji, skoro każdorazowo wymagają czynności wykonywanej osobiście. W przypadku usługi, która trwa przez pewien czas, jednorazowa, osobista płatność wymaga odseparowania jej od usługi. Albo płatność za całość usługi opłacający wnosi z góry, biorąc na siebie całe ryzyko nieskorzystania z usługi, bo okazała się ona niedostępna, albo z dołu, ale wówczas ryzyko niezapłacenia za usługę przez usługobiorcę jest w całości po stronie odbiorcy płatności, który jest zmuszony uwzględnić je w cenie usługi. Dla przykładu, bilety transportu miejskiego kasujemy w momencie wejścia do pojazdu – jeśli ten pojazd się zepsuje lub stanie w korku, to usługa nie jest zrealizowana, ale prawdopodobieństwo, że pasażer odzyska pieniądze za niezrealizowaną usługę, jest małe.

Usługi z płatnościami częściowymi lub wycofywaniem opłat po niezrealizowaniu usługi w całości są bardzo niechętnie przyjmowane przez usługobiorców i generują szereg problemów. Dla przykładu, poznańska elektroniczna karta aglomeracyjna PEKA, podobnie jak londyńska karta Oyster, w momencie wejścia pasażera do pojazdu komunikacji publicznej pobiera opłatę za trasę do ostatniego przystanku, a w momencie wyjścia z pojazdu na wcześniejszym przystanku, po stwierdzeniu faktu przyłożenia karty do czytnika, zwraca cenę niewykorzystanych przystanków [PEKA 2020, TFL 2020b]. Jeśli czytnik ulegnie awarii albo jeśli wystąpi błąd komunikacji z serwerem, to pasażer ponosi całe ryzyko (i koszty), a możliwość reklamacji w takiej sytuacji jest mocno ograniczona.

Zwróćmy uwagę, że w opisanym powyżej sposobie realizacji usługi to płatność jest tym elementem, który najbardziej wpływa na zaufanie i zadowolenie obu stron. Jeśli usługa nie zostanie zrealizowana, ale płatność nie będzie naliczona, płatnik w większości przypadków nie będzie miał pretensji do usługodawcy. Jednak pasażer komunikacji publicznej, który zapłacił za bilet, a potem został zmuszony do spaceru po awarii pojazdu, będzie miał pretensje nie do kierowcy, tylko



do usługodawcy, który nie zwrócił mu kosztów niewykorzystanego biletu. Podobnie działa efekt niezrealizowania przedpłaconej usługi – na przykład osoby, które wykupiły bilety kwartalne lub półroczne w lutym 2020 roku i nie mogły korzystać z usług transportu publicznego ze względu na epidemię koronawirusa, zgłaszają (w ich mniemaniu słuszne) reklamacje, choć nie zawsze istnieją podstawy prawne do zwrotu opłaty, bo na przykład nie przewiduje tego regulamin.

Usługi, w których zakłada się wprowadzanie opłat proporcjonalnych do ich użycia, wymagają wcześniejszej rejestracji w systemie płatności za tę konkretną usługę. Jeśli, jak się przewiduje, wkrótce liczba usługodawców w inteligentnych miastach zacznie być liczona w setkach, a nawet tysiącach, to takie rejestracje będą niepraktyczne.

Przykładowo, w Poznaniu funkcjonuje wielu usługodawców oferujących usługi z zakresu transportu rozliczanego na minuty (np. nextbike, blinker.city, hop.city, lime, Traficar, 4mobility, Panek CarSharing, easyshare, Click2Go). Czynność rejestracji wymaga założenia konta użytkownika i określenia hasła dostępu – z punktu widzenia przeciętnego użytkownika posiadanie wielu takich kont sprawia duże problemy organizacyjne, problemy w zapamiętywaniu stanu kont przedpłaconych oraz haseł, a także pośrednio powoduje spadek bezpieczeństwa (jeśli dana osoba stosuje dla wygody to samo hasło w wielu miejscach). Każda rejestracja to także konieczność spełnienia wymagań dotyczących ochrony danych osobowych [Ustawa 2019/1781] oraz potencjalne miejsce utraty prywatności, jeśli dane zebrane na rzecz lub podczas świadczenia usługi dostaną się w niepowołane ręce. Z tego względu uniknięcie potrzeby rejestracji u każdego usługodawcy z punktu widzenia obu stron staje się bardzo ważne. Tu pojawia się szczególna rola banku, jako podmiotu budującego zaufanie między stronami płatności. Na takiej samej zasadzie, jak dzisiaj dokonujemy zakupów bez potrzeby osobnej rejestracji w każdym sklepie używając karty płatniczej wydanej przez bank, powinno ograniczyć się konieczność rejestracji usługobiorcy u każdego usługodawcy z osobna do jednorazowej rejestracji w systemie płatności strumieniowych w banku, ewentualnie cyklicznie odnawiając pewne uprawnienia.

W inteligentnych miastach, których infrastruktura ma ograniczoną pojemność i cechuje się ograniczoną elastycznością w odpowiedzi na rosnącą populację, efektywne świadczenie usług wiąże się z koniecznością wprowadzenia cen elastycznie zmieniających się w zależności od popytu na daną usługę [Deloitte 2015b]. Cena zostaje wtedy wykorzystana do stymulowania zachowania konsumentów danej usługi, aby odpowiednio zachęcić lub zniechęcić ich do jej konsumpcji

[Yamabe i inni 2010]. Dynamicznie wyznaczane ceny znajdują zastosowanie w takich obszarach inteligentnego miasta, jak ograniczenie zatłoczenia dróg oraz przestrzeni publicznych (wysokość opłaty parkingowej zależna od liczby wolnych miejsc, wysokość opłaty za przejazd komunikacją miejską uzależniona od liczby wolnych miejsc), a także ograniczenie zanieczyszczenia gazami cieplarnianymi (wysokość opłaty za wjazd do miasta uzależniona od pory dnia, zatłoczenia, szybkości przemieszczania się) [Deloitte 2017]. Płatności strumieniowe pozwalają na płacenie za usługi, których cena zmienia się często w czasie, przy czym umożliwiają zmianę ceny usługi w trakcie jej świadczenia w sposób akceptowalny dla obu stron – płatnika i odbiorcy płatności.

3.3. Klasyfikacja opłat za usługi w inteligentnym mieście

Płatności za usługi w inteligentnym mieście można sklasyfikować w kontekście pikopłatności strumieniowych według następujących kryteriów:

- 1) ze względu na sposób wnoszenia opłat,
- 2) ze względu na liczbę i powtarzalność interakcji,
- 3) ze względu na rozłożenie w czasie lub przestrzeni,
- 4) ze względu na wysokość wnoszonych opłat.

Ze względu na sposób wnoszenia opłat możemy podzielić płatności za usługi na:

- opłacane bezpośrednio na rzecz podmiotu gospodarczego, w tym komunalnego – na przykład opłaty za transport publiczny (tramwaje, autobusy, rowery miejskie), ale także taksówki i hulajnogi, opłaty za naładowanie samochodu elektrycznego, opłaty za skorzystanie z ośrodków sportowych i kulturalnych (kina, teatry, muzea, parki rozrywki) oraz opłaty za dostęp do sieci (energetycznej, telekomunikacyjnej, informatycznej);
- opłacane bezpośrednio na rzecz jednostki administracji – na przykład opłaty środowiskowe, klimatyczne, za gospodarkę odpadami itp.;
- opłacane pośrednio przez operatora płatności – na przykład opłaty za parking miejski, pobierane przez wyznaczonego operatora tego parkingu, opłaty za zwiedzenie galerii, wystaw itp.;
- bezpłatne, czyli opłacane z podatków (na przykład tablice informacyjne z rozkładem jazdy autobusów i tramwajów).

Ze względu na liczbę i powtarzalność interakcji możemy podzielić płatności za usługi na:

- jednorazowe,
- powtarzalne (na przykład częste przejazdy komunikacją miejską, wielokrotne parkowanie na tym samym parkingu itp.).

Ze względu na rozłożenie usług w czasie wyróżniamy:

- płatności za usługi krótkotrwałe (na przykład odwiedzenie punktu widokowego),
- płatności za usługi rozłożone w czasie (na przykład pełne ładowanie samochodu elektrycznego, co zabiera odpowiednio dużo czasu, przejazd autobusem na trasie obejmującej kilka przystanków, dłuższe parkowanie itp.). W tym przypadku naliczenie opłaty za usługę zależy od liczby jednostek czasu trwania usługi (np. liczba minut, w czasie których użytkownik korzystał z roweru miejskiego), natomiast wielkość jednostki zależy od rodzaju usługi.

Z punktu widzenia korzyści z wprowadzenia automatyzacji usług, można dostrzec szczególny potencjał usług powtarzalnych i długotrwałych. Realizacja płatności w przypadku takich usług jest, przy wykorzystaniu dzisiejszych narzędzi, sporym wyzwaniem. Po pierwsze, powtarzalność usługi rzadko oznacza także powtarzalność płatności. O ile sama usługa może być zautomatyzowana, o tyle płatność wymaga każdorazowego zaangażowania użytkownika w proces płatności lub opłaty subskrypcyjnej wnoszonej z góry. Po drugie, długotrwałość usługi zwiększa poziom ryzyka: w przypadku opłaty z góry – dla płatnika, który nie jest pewny, czy wykorzysta usługę w całym opłaconym okresie, natomiast w przypadku opłaty z dołu, po zrealizowaniu usługi – dla odbiorcy płatności, który nie jest pewien otrzymania zapłaty. Im dłużej świadczona jest usługa, tym większy jej koszt, a zatem tym większe ryzyko dla jednej ze stron.

Wspomniana opłata subskrypcyjna, która jest zwykle wnoszona tylko na rzecz wybranej usługi, oraz konieczność rejestracji zniechęca do sporadycznego korzystania z usługi. Dla osoby przebywającej w mieście – na stałe lub sporadycznie – dobrym rozwiązaniem jest dostęp do uniwersalnego systemu płatności, za pomocą którego po jednorazowym zarejestrowaniu się mógłby płacić za wszystkie usługi w sposób automatyczny.

W przypadku płatności za usługi konsumowane sporadycznie, wcześniejsza rejestracja u usługodawcy nie jest uzasadniona. Zatem także w tym przypadku integracja na poziomie sposobu płatności jest bardzo

pożądana – dopiero taka integracja umożliwi praktyczną realizację tego typu płatnych usług w trybie całkowicie automatycznym.

W przypadku klasyfikacji ze względu na wartość usługi, wyróżniamy z jednej strony makropłatności, a z drugiej – mikro- i pikopłatności. W przypadku makropłatności kwota rozliczenia za usługę jest na tyle wysoka, że opłacalne jest stosowanie standardowych metod rozliczeń bankowych, w szczególności przelewów, płatności kartą i Blikiem. W przypadku mikropłatności, opiewających często na kwoty groszowe, stosowanie standardowych metod rozliczeń bankowych jest nieopłacalne, a w przypadku pikopłatności dopuszczających ułamki grosza – niemożliwe. Rozwiązaniem jest agregacja płatności, czyli ich zsumowanie w dłuższym czasie i uregulowanie za pomocą jednej standardowej makropłatności. Klasyczna agregacja obejmuje rozliczenie mikro- lub pikopłatności jednego usługodawcy. W przypadku wielu usługodawców operujących w przestrzeni miasta jest to zatem rozwiązanie niezbyt użyteczne. Dlatego proponujemy taki sposób agregacji płatności, który uwzględnia wielu usługodawców (odbiorców płatności) i obejmuje dowolne kwoty.

3.4. Potencjał rozwoju płatnych usług automatycznych

W świetle powyższych rozważań pojawia się pytanie, dla jakich typów usług jest wymagany system pikopłatności strumieniowych, aby umożliwić ich pełną automatyzację? Klasyczne usługi, rozliczane oświadczeniem woli i jednorazową transakcją płatniczą opiewającą na większą kwotę, nie będą podlegać pełnej automatyzacji w najbliższym czasie. Dla przykładu, tankowanie samochodu na stacji benzynowej, rozliczane na podstawie wskazań dystrybutora, pozostanie przypuszczalnie w niewiele zmienionej formie ze względu na przyzwyczajenia i istniejącą infrastrukturę. Należy jednak zauważyć, że nawet tu są stopniowo wprowadzane zmiany, np. aplikacja mobilna Orlen Pay [Orlen 2020].

Jednak już ładowanie samochodu elektrycznego, szczególnie w miejscach, które do tej pory nie kojarzyły się z tą czynnością (np. na wybranych miejscach parkingowych), wymaga usprawnienia. W chwili obecnej ładowanie samochodu wymaga podłączenia wtyczki oraz włożenia karty płatniczej do czytnika w celu dokonania najpierw rezerwacji płatności, a następnie samej płatności. Jednak gdy rozpowszechnią się ładowarki indukcyjne, takie rozwiązanie będzie niepraktyczne. Częściowym rozwiązaniem byłaby aplikacja w smartfonie, którą kierowca uaktywniałby po zaparkowaniu samochodu nad taką ładowarką w celu rozliczenia transakcji. Jednakże proces takiego rozliczenia podlegałby automatyzacji w minimalnym stopniu – wszystkie czynności



musiałby wykonać właściciel telefonu, podobnie jak obecnie w aplikacji Orlen Pay.

Zdecydowanie lepsza byłaby sytuacja, w której właściciel pojazdu deklaruje, w jakiej maksymalnej cenie (lub poniżej jakiego poziomu energii w akumulatorach) jest zdecydowany ładować baterie, czyli kupować energię. Wykryty w nawierzchni jezdni czujnik ładowania inicjowałby automatycznie dwa procesy: przekazywania energii i płatności strumieniowych – wszystko w sposób całkowicie automatyczny, bez potwierdzania kolejnych czynności przez człowieka. Kierowca tylko zatrzymałby pojazd nad ładowarką, a po pewnym czasie odjechał. Oczywiście do rozwiązania pozostają problemy niezawodności transmisji oraz wzajemnego zaufania między dostawcą energii a kierowcą – niniejszy raport wskazuje stosowne rozwiązanie w tym zakresie.

Należy zauważyć, że powyższy sposób realizacji usługi można uogólnić. Na takiej samej zasadzie, jak opisana powyżej, można podładować telefon komórkowy siedząc na ławce w parku lub jadąc autobusem. Jeśli te miejsca są wyposażone w ładowarki indukcyjne, położenie smartfonu we właściwej pozycji rozpoczyna ładowanie, a wzięcie z powrotem do ręki – kończy. Proces ładowania telefonu różni się od ładowania samochodu elektrycznego właściwie tylko ilością przekazanej energii, a w konsekwencji – kwotą rozliczenia. Jednakże ta różnica we wskazanym przypadku jest znaczna – od kilkunastu złotych za pełne ładowanie samochodu w czasie kilku godzin do ułamków grosza za ładowanie telefonu w ciągu kilku minut jazdy autobusem. Proponowany w tym opracowaniu system pikopłatności strumieniowych AMFI uwzględnia nawet tak dużą skalę kwotową w pełni automatycznych rozliczeniach.

Ze względów opisanych powyżej, głównie z powodu konieczności rejestracji u usługodawcy i niskich opłat za usługi, w klasycznym ujęciu nie opłaca się proponować płatnych usług sporadycznych opiewających na bardzo małe kwoty.

W proponowanym systemie pikopłatności strumieniowych wręcz przeciwnie – takie usługi, które w masie będą przypuszczalnie generować bardzo duży ruch, mogą być bardzo ważnym obszarem aplikacyjnym. W ten obszar wpisują się nie tylko klasyczne automaty do wydawania przekąsek i napojów, ale także na przykład urządzenia do pobierania niewielkich opłat za przejazd, przejście lub postój, które automatycznie naliczają opłaty za rzeczywisty czas użycia danego zasobu. Automatyzacja w systemie AMFI znacznie zwiększa wygodę korzystania z takich usług, gdyż nie wymaga bezpośredniego zaangażowania klienta w proces płatności. Dla przykładu, w klasycznym ujęciu, podjeżdżając

samochodem do szlabanu blokującego wjazd na parking, musimy otworzyć szybę i okazać kartę płatniczą – dopiero weryfikacja płatności spowoduje podniesienie szlabanu. Podobnie jeśli płacimy za pośrednictwem aplikacji w smartfonie – musimy tę aplikację uruchomić i wprowadzić/wybrać dane dla celów konkretnej płatności. W odróżnieniu od powyższych rozwiązań, AMFI nie wymaga okazywania karty ani smartfonu – klient jedynie korzysta z usługi, nie dbając osobiście o procedurę zapłaty, jeśli uprzednio wyraził zgodę na automatyczne płacenie za pomocą AMFI danemu usługodawcy.

3.5. Zalety pikopłatności strumieniowych dla usługodawców

Od dłuższego czasu obserwujemy dążenie usługodawców do automatyzacji świadczonych usług. Zastosowanie technologii informacyjnych, w szczególności mobilnych, pozwala na optymalizację procesów zarówno ze względu na czas, jak i na koszt przetwarzania danych. Płatności są procesem jeszcze nie w pełni zautomatyzowanym. O ile proces rozliczeń finansowych po stronie usługodawcy jest praktycznie w całości zautomatyzowany, o tyle sama realizacja płatności po stronie usługobiorcy wymaga wielu manualnych czynności z jego strony. Dla przykładu, klient może kupić bilet sieciowy komunikacji miejskiej, ale musi w tym celu odszukać stronę przedsiębiorstwa komunikacyjnego, założyć konto na serwerze operatora miejskiej sieci transportowej, a następnie zasilić je środkami pieniężnymi. W praktyce, należy te czynności wykonać dla każdej usługi, a co najmniej każdego usługodawcy. W efekcie, takie skomplikowane procedury odstraszały klientów od usług – klienci ograniczają się do usług, które naprawdę uznają za niezbędne. Usługodawcy z pewnością byłiby zainteresowani wprowadzaniem na rynek nowych usług, które nie wymagałyby rejestracji i manualnych przelewów, a co za tym idzie – przyciągnęły nowych klientów.

Przeniesienie automatyzacji płatności w formie pikopłatności strumieniowych na bank z przeznaczeniem potencjalnie dla wszystkich usługodawców uwolniłoby nowe rynki usług. W szczególności dotyczy to usługodawców, którzy działają w małej skali i którzy nie chcą inwestować w skomplikowany system rozliczeniowy. Dla przykładu, sieć ładowania samochodów elektrycznych obsługiwana przez jednego dużego operatora (tak jak dzisiejsze sieci stacji benzynowych) można by uzupełnić mikroładowarkami indukcyjnymi, instalowanymi na miejscach parkingowych przy prywatnych posesjach lub sklepach i zasilanych energią z paneli słonecznych na dachu najbliższego budynku. Każda z takich niewielkich ładowarek byłaby własnością niezależnego przedsiębiorcy, w tym mikroprzedsiębiorcy, który, poza samą stacją ładowania, nie musi utrzymywać dodatkowej infrastruktury niezbędnej do realizacji płatności za

usługę – rolę pośrednika może, jak wskazuje niniejsze opracowanie, przejąć bank, bez konieczności instalacji urządzeń typu POS.

3.6. Zalety pikopłatności strumieniowych dla usługobiorców

Praktycznie wszyscy klienci bardzo cenią sobie wygodę zakupów. System pikopłatności strumieniowych może tę wygodę znacznie zwiększyć. Zamiast szukać parkometru i ryzykować starcie z kontrolerem, lepiej po prostu zaparkować samochód, a potem odjechać w dowolnym momencie – samochód w połączeniu ze smartfonem sam zadba o strumieniowe wniesienie opłaty za wykorzystany czas na parkingu.

Jest rzeczą powszechnie znaną, że klienci nie tylko chcą uwolnić się od rutynowych czynności typu okazywanie karty bankowej, ale także pragną przerzucić jak najwięcej czynności na swój smartfon. Jeśli do tego dodamy kontrolę automatycznych wydatków typu ograniczenie sumy miesięcznych wydatków, miejsc, w których chcemy korzystać z usług, ich typu, poziomu zaufania (np. ufamy tylko tym usługodawcom, którzy uprzednio uzyskali stosowny certyfikat) itp., a także cykliczne raportowanie i ostrzeganie o „krytycznych” i „niebezpiecznych” transakcjach w czasie rzeczywistym, to otrzymamy bardzo efektywne i wygodne narzędzie rozliczania praktycznie dowolnych usług w ten sam sposób, czyli produkt skierowany do wszystkich osób przebywających w inteligentnym mieście.

3.7. Zalety pikopłatności strumieniowych dla banków

Wprowadzenie pikopłatności pociąga za sobą szereg korzyści dla obsługujących je banków. Po pierwsze, ten sposób płatności pozwala na przejęcie obsługi płatności, które do tej pory były zarezerwowane wyłącznie dla gotówki. Ponadto pikopłatności pozwalają na rozliczanie opłat na kwoty poniżej jednego grosza, co przy skumulowanym efekcie „długiego ogona” (ang. long tail) niskokwotowych i masowych płatności pozwoli na zagospodarowanie obecnej luki w płatnościach, przez objęcie obowiązkiem zapłaty większej liczby przypadków.

Po drugie, pikopłatności mogą być interesującą alternatywą dla kart płatniczych i rozliczeń BLIK, przez eliminację oświadczenia woli i całkowity automatyzm płatności po obu stronach. Automatyzm zwiększy wygodę z punktu widzenia płaconego, a co za tym idzie – powiększy wolumen takich płatności. Taka zmiana wymaga stosunkowo niewielkich inwestycji po stronie banków i nie narusza obecnych sposobów rozliczeń.

Po trzecie, pikopłatności mogą przejąć część rynku do tej pory zarezerwowanego dla podmiotów pozabankowych typu mPay. Takie przejście będzie z dodatkową korzyścią dla klientów, którzy oprócz wygody wynikającej z automatyzacji płatności po ich stronie, uzyskają także możliwość wykorzystania uniwersalnego sposobu wnoszenia opłat bez konieczności rejestracji konta u wielu pośredników.

Potencjalny zysk z obrotu pikomonetami dla banku leży w możliwości wprowadzenia szerokiego spektrum opłat i prowizji, zarówno od płatnika, jak i od odbiorcy płatności. Dla przykładu, opłatą mogą być objęte: wydanie pieniądza elektronicznego, fakt inicjacji płatności, rozliczenie dokonywane odbiorcy płatności itp. Opłatą może być też procent od wartości zagregowanych płatności, wnoszony przez ich odbiorcę.

Bank w proponowanym rozwiązaniu staje się uniwersalnym pośrednikiem w nowym rodzaju płatności i jest postrzegany jako centrum nowoczesnych rozwiązań, co będzie odebrane jako powtórzenie sukcesu BLIK i płatności zbliżeniowych. Jednocześnie fakt płatności pikomonetami przestanie być kojarzony z przykrym obowiązkiem na rzecz banku, a przez zwiększenie stopnia wygody korzystania stanie się dostępny także dla wielu nowych grup klientów, którzy nie radzili sobie z płatnościami kartą lub kodami BLIK.

3.8. Uzasadnienie potrzeby pikopłatności strumieniowych

W świetle powyższych sekcji tego rozdziału można podsumować ogólne cechy systemu pikopłatności strumieniowych:

- 1) *Możliwość automatyzacji płatności* po stronie usługobiorcy, a nie tylko usługodawcy;
- 2) *Uniwersalność*, rozumiana jako możliwość zastosowania zarówno do usług jednorazowych i długotrwałych niezależnie od charakteru tych usług;
- 3) *Wygoda*, rozumiana jako brak potrzeby rejestracji usługobiorcy u każdego usługodawcy niezależnie – usługobiorca uaktywnia system pikopłatności strumieniowych na swoim rachunku osobistym w banku;
- 4) *Skalowalność*, rozumiana jako możliwość dokonywania zarówno piko-, mikro-, jak i makropłatności za pomocą tego samego systemu, na zasadach uzgadnianych między usługobiorcą a usługodawcą,
- 5) *Równomierne rozłożenie ryzyka* na obie strony płatności: usługobiorcę i usługodawcę.



Cechy systemu pikopłatności strumieniowych AMFI



Cecha 1: Zapewnienie ostatecznego rozliczenia transakcji

System pikopłatności strumieniowych AMFI zapewnia ostateczne rozliczenie płatności dokonanych za pomocą pieniądza elektronicznego.

Uzasadnienie

Wykorzystując gwarancje banków wydających pieniądź elektroniczny, odbiorcy płatności mają pewność, że otrzymany od płatników pieniądź elektroniczny zostanie rozliczony przez banki i zamieniony na pieniądź fiducyjny.

Cecha 2: Zapewnienie bezpieczeństwa obrotu środkami płatniczymi

System pikopłatności strumieniowych AMFI zapewnia bezpieczeństwo wykorzystywanych środków płatniczych.

Uzasadnienie

Banki jako podmioty podlegające ścisłemu nadzorowi ze strony państwa i banku centralnego są gwarantem bezpieczeństwa obrotu środkami płatniczymi. Ochronie podlega wszelka forma pieniądza, zarówno po stronie płatnika (niewykorzystane środki płatnicze), jak i odbiorcy płatności (zarówno środki wymienione na pieniądź fiducyjny, jak i oczekujące na tę wymianę).

Cecha 3: Obsługa strumienia pikopłatności

System pikopłatności strumieniowych AMFI jest tak skonstruowany, aby w czasie technicznej realizacji strumienia pikopłatności nie był wymagany udział innych podmiotów niż płatnik i odbiorca płatności.

Uzasadnienie

Po zainicjowaniu z udziałem banku płatnika strumienia pikopłatności między płatnikiem i odbiorcą płatności nie wymaga on udziału żadnych podmiotów pośredniczących. Brak pośredników jest konieczny ze względu na spodziewaną dużą liczbę jednoczesnych pikopłatności w przestrzeni inteligentnego miasta. Brak pośredników likwiduje też pozabankowe koszty transakcji.

Cecha 4: Umożliwienie płatności sporadycznych

Płatność sporadyczna jest możliwa wówczas, gdy każdy płatnik posiadający pieniądź elektroniczny ma możliwość zainicjowania strumienia pikopłatności w dowolnym momencie z dowolnym odbiorcą płatności

akceptującym ten pieniądź elektroniczny bez konieczności dodatkowej komunikacji z innymi podmiotami niż odbiorca płatności. Ze strony płatnika nie jest też wymagana wcześniejsza rejestracja u odbiorcy płatności.

Uzasadnienie

Inteligentne miasto stanowi środowisko zróżnicowane i dynamicznie zmieniające się. Mamy w nim do czynienia z osobami często i na masową skalę przyjeżdżającymi do niego, przebywającymi w nim przez jakiś czas i wyjeżdżającymi z niego. Osoby te są wyposażone w różne smartfony i inne urządzenia elektroniczne oraz korzystają z różnego oprogramowania i różnych aplikacji. Obszar miasta to potencjalnie miejsce na bardzo dużą liczbę usług, oferowanych przez wielu usługodawców, czyli potencjalnych odbiorców płatności. Ze względu na dużą zmienność, usługobiorcy często nie nawiązują długotrwałych relacji z usługodawcami. Dlatego system pikopłatności powinien umożliwiać płatności sporadyczne.

Cecha 5: Odporność na zerwanie komunikacji

Strumień pikopłatności strumieniowych AMFI jest odporny na zerwanie komunikacji między płatnikiem i odbiorcą płatności. Jeśli zainicjowany strumień pikopłatności oraz świadczenie usługi zostaną zakończone po pewnym czasie ze względu na zerwanie komunikacji, to płatnik zostanie obciążony na rzecz odbiorcy płatności kwotą nie większą niż to wynika z faktycznie dokonanych pikopłatności, odpowiadającą faktycznemu okresowi korzystania z usługi, poprzedzającemu zerwanie transmisji.

Uzasadnienie

W inteligentnym mieście będzie dochodzić do sytuacji zrywania komunikacji między usługobiorcą a usługodawcą, ze względu na wyjście urządzenia usługobiorcy z zasięgu lokalnej sieci, np. po wyjściu z budynku, placu zabaw lub tramwaju lub awarię komunikacji. Taka sytuacja powinna być traktowana jako zakończenie świadczenia usługi i nie powinna wpływać na wcześniej zrealizowane płatności, których wartość jest proporcjonalna do czasu od początku do momentu przerwania świadczenia usługi.

Cecha 6: Zapewnienie anonimowości płatnika

Protokół pikopłatności w systemie AMFI chroni anonimowość płatnika, co oznacza, że dane wymagane do zainicjowania i realizacji strumienia pikopłatności nie ujawniają tożsamości płatnika żadnemu podmiotowi.



Uzasadnienie

W inteligentnym mieście będzie duża liczba usługobiorców jednocześnie korzystających z różnych usług oferowanych przez wielu usługodawców. Stanowi to potencjalne zagrożenie dla zachowania prywatności usługobiorców. System pikopłatności strumieniowych AMFI, dzięki zastosowaniu protokołów kryptograficznych, technicznie zapewnia anonimowość płatników.

Cecha 7: Odporność na fałszerstwo pieniądza elektronicznego

Pieniądz elektroniczny używany w systemie pikopłatności strumieniowych AMFI jest odporny na fałszowanie, czyli niemożliwe jest wytworzenie fałszywego pieniądza elektronicznego, który byłby uznany za prawdziwy przez wydawcę pieniądza elektronicznego, lub zaakceptowany przez dowolnego odbiorcę płatności.

Uzasadnienie

Podobnie jak w przypadku papierowych banknotów, które są trudne do podrobienia dzięki unikalnej technologii produkcji, pieniądz elektroniczny musi być wydawany z zastosowaniem zaawansowanych algorytmów, które uniemożliwią jego wydawanie przez podmioty nieuprawnione. Pieniądz elektroniczny musi być zabezpieczony za pomocą technik kryptograficznych, które na podstawie unikalnych kluczy szyfrujących oraz metod weryfikacji skutecznie zabezpieczą go przed fałszerstwem. Skuteczność zabezpieczenia pieniądza elektronicznego dzięki współczesnym, długim, losowym kluczom szyfrującym pozwala uodpornić pieniądz elektroniczny przed fałszerstwem lepiej niż unikalne, precyzyjne techniki poligraficzne stosowane w produkcji pieniądza papierowego.

Cecha 8: Odporność na nieuprawnione wielokrotne użycie pieniądza elektronicznego

Płatnik może użyć danego pieniądza elektronicznego do wyłącznie jednej płatności wobec wyłącznie jednego odbiorcy.

Uzasadnienie

Mimo tego, że pieniądz elektroniczny można łatwo skopiować, a kopia jest identyczna z oryginałem, system pikopłatności strumieniowych AMFI zapewnia, że można ten pieniądz wydać tylko jeden raz. Każda próba zapłaty pieniądzem elektronicznym po raz drugi i następny skończy się odrzuceniem płatności.

Cecha 9: Uniwersalność

System pikopłatności strumieniowych AMFI może być zastosowany przez dowolnego usługodawcę do każdej świadczonej przez niego usługi.

Uzasadnienie

System pikopłatności strumieniowych AMFI umożliwia każdemu płatnikowi zapłacenie za usługi oferowane przez odbiorcę płatności, nawet w przypadku bardzo niskiej kwoty pojedynczej płatności.

Cecha 10: Skalowalność

System pikopłatności strumieniowych AMFI umożliwia rozliczanie opłat za usługi na kwoty opiewające od ułamków grosza do dowolnie wyznaczonej górnej granicy kwotowej płatności elektronicznych, wynikającej z regulacji prawnych albo regulaminu banku.

Uzasadnienie

System pikopłatności strumieniowych AMFI w taki sam sposób rozlicza zarówno pojedyncze pikopłatności na bardzo drobne kwoty, jak i strumień płatności składający się na większą makroopłatę za korzystanie z usługi (np. przez długi czas). System agreguje pikopłatności zarówno po stronie płatnika (do celów zarządzania kontem i pozostałymi środkami pieniężnymi), jak i po stronie odbiorcy płatności (do celów wymiany na pieniądz fiducjarny).

Cecha 11: Automatyzm

W systemie pikopłatności strumieniowych AMFI strumień pikopłatności odpowiadający rozliczeniu finansowemu usługi jest rozliczany automatycznie po obu stronach. W szczególności, nie jest wymagane potwierdzenie każdej pikopłatności ze strony płatnika, pod warunkiem zadeklarowania przez niego wcześniej maksymalnych rozliczanych kwot (lub innych ograniczeń, w tym miejsca i czasu transakcji, typów opłacanych usług, wymaganego poziomu zaufania do odbiorcy płatności itp.) oraz wykorzystania stosownych metod budowy zaufania do usług.

Uzasadnienie

Pikopłatności realizowane w ramach strumienia w krótkich odstępach czasowych (nawet rzędu ułamka sekundy) nie mogą wymagać potwierdzania każdej pikopłatności przez człowieka. Z tego powodu za potwierdzanie płatności musi być odpowiedzialna aplikacja płatnika, który zaakceptował wcześniej ogólne reguły płatności (np. maksymalne kwoty, dozwolone miejsca i typy świadczonych usług, akceptowane podpisy elektroniczne usługodawców i odbiorców płatności itp.), analogicznie do polecenia zapłaty.



Architektura systemu pikopłatności w inteligentnym mieście



W tym rozdziale opisano architekturę systemu anonimowych pikopłatności strumieniowych AMFI za usługi świadczone w inteligentnych miastach.

Przeznaczenie systemu AMFI

System strumieniowych pikopłatności AMFI jest przeznaczony do pobierania opłat za usługi w inteligentnym mieście. Opłaty są proporcjonalne do czasu świadczenia usługi. Opłaty mogą być pobierane automatycznie, bez konieczności wykonywania bezpośrednich manualnych operacji przez usługobiorcę. Schemat systemu AMFI ilustruje Rysunek 2. W systemie AMFI funkcjonują liczne podmioty pełniące role różnych aktorów systemu. Bank może być zarówno wydawcą pieniądza elektronicznego, jak i świadczyć usługę rozrachunku dla odbiorców płatności.

Neutralność ekonomiczna

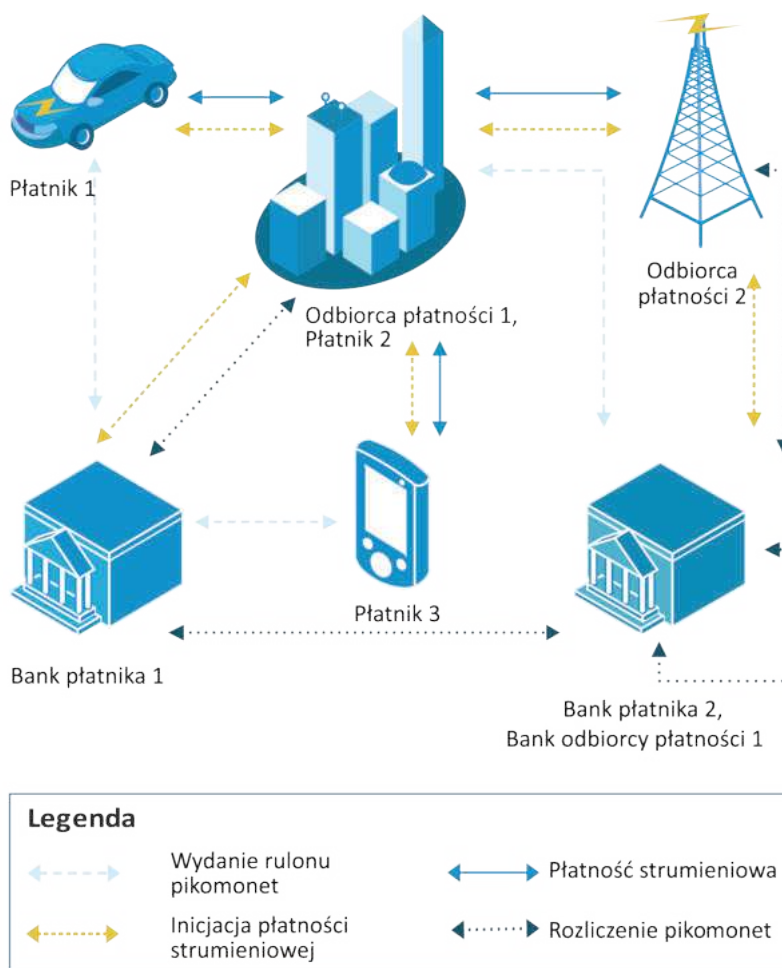
Rozwiązania techniczne zastosowane w systemie AMFI są neutralne ekonomicznie, gdyż dają dużą swobodę w zakresie ustalania nominałów oraz sposobu rozliczania przez banki pikopłatności. Poniżej

przedstawiono cechy systemu, które stanowią o jego neutralności ekonomicznej.

- System AMFI nie jest propozycją kolejnej kryptowaluty, lecz umożliwia dokonywanie płatności denominowanych w walucie krajowej.
- Zestaw reguł płatności może być elastycznie dostosowywany przez odbiorcę płatności w zależności od konkretnego płatnika. W szczególnym przypadku płatnik i odbiorca płatności mogą określić zestaw reguł płatności w drodze negocjacji poza system AMFI.
- Pikomonety utworzone w systemie AMFI mogą mieć wartość mniejszą niż najmniejsza jednostka waluty.

Wielość uczestników systemu

System AMFI pozwala na współistnienie wielu podmiotów działających jako płatnicy (usługobiorcy), odbiorcy płatności (usługodawcy) i banki (wydawcy pieniędzy elektronicznych). Każdy podmiot, który chce działać jako płatnik, odbiorca płatności lub bank i spełnia wymogi prawne, może dołączyć do systemu AMFI.



Rysunek 2. Poglądowy schemat system AMFI

Anonimowość płatnika

W systemie AMFI płatnik nie jest zmuszony do ujawnienia swojej tożsamości podczas dokonywania pikopłatności. Jest to możliwe, ponieważ to bank płatnika, a nie płatnik, jest podmiotem odpowiedzialnym za przekazywanie środków do odbiorcy. W systemie AMFI zastosowano techniki kryptograficzne (kryptograficzny protokół ślepych podpisów) do utajnienia związku między identyfikatorem rulonu pikomonet a tożsamością płatnika. Chociaż system AMFI nie ujawnia tożsamości płatnika, w wyjątkowych sytuacjach, w celu świadczenia usługi, odbiorca płatności może wymagać od płatnika ujawnienia tożsamości lub innej formy uwiarygodnienia, związanej z podaniem pewnych danych wrażliwych lub osobistych. Dla przykładu, przyznanie zniżki dla osób niepełnosprawnych wymaga udowodnienia, że jest się taką osobą, należy zdradzić swój wiek, żeby uzyskać rabat dla osób starszych itp. Są to sytuacje specyficzne dla konkretnej usługi.

Przejrzystość banku i odbiorcy płatności

Podmioty działające jako odbiorcy płatności lub wydawcy elektronicznego pieniądza muszą posiadać certyfikaty klucza publicznego. Odbiorca płatności jest usługodawcą, który musi ponosić odpowiedzialność za jakość świadczonych usług. Dlatego płatnik musi znać tożsamość odbiorcy, aby móc dochodzić swoich praw. Natomiast bank płatnika bierze na siebie odpowiedzialność za obsługę operacji finansowych. Dlatego jego tożsamość musi być znana zarówno płatnikowi, jak i odbiorcy.

Zapobieganie oszustwom

System AMFI jest zaprojektowany w sposób zabezpieczający przed próbą oszustwa ze strony każdego podmiotu zaangażowanego w pikopłatność strumieniową. Bank płatnika jest odpowiedzialny za swoje działania i podlega nadzorowi ze strony KNF. System AMFI uniemożliwia płatnikowi odniesienie korzyści z działań niezgodnych z protokołami. W przypadku, gdyby płatnik próbował wydać więcej pikomonet niż zawarte w zakupionym przez niego rulonie pikomonet, to dodatkowe pikomony nie będą akceptowane. W przypadku, gdyby płatnik próbował wielokrotnie zapłacić tymi samymi pikomonetami wielu odbiorcom, to jest to niemożliwe, gdyż bank płatnika blokuje możliwość skierowania strumienia pikopłatności do wszystkich odbiorców płatności z wyjątkiem pierwszego, na rzecz którego płatnik zainicjował strumień.

Teoretycznie odbiorca płatności może odmówić świadczenia usługi po rozpoczęciu otrzymywania pikopłatności od płatnika, choć naraża go to na utratę wiarygodności. W takiej sytuacji płatnik może wyjść z zasięgu sieci, przez którą są przekazywane

pikopłatności lub ręcznie zatrzymać strumień pikopłatności wychodzący z jego urządzenia.

Nieuczciwy płatnik i odbiorca płatności, nawet jeśli współpracują ze sobą, nie mogą podrabiać ani wielokrotnie wydawać pikomonet. Baza danych rulonów pikomonet wraz z mechanizmem blokującym zapobiega podwójnemu wydatkowaniu pikomonet, zatem sfałszowanie pikomonet byłoby teoretycznie możliwe tylko po kradzieży kryptograficznego klucza prywatnego banku płatnika.

Urządzenia płatników

System AMFI nadaje się do instalacji na lekkich, przenośnych urządzeniach płatników, które cechują się małą mocą obliczeniową i pojemnością pamięci, takich jak smartfony. System nie wymaga, aby płatnik łączył się z bankiem – wydawcą elektronicznego pieniądza – podczas płatności strumieniowej. Połączenie między płatnikiem a odbiorcą nie musi być nawiązywane przez internet, tylko na przykład przez Bluetooth, NFC itp.

Dany płatnik może korzystać z modułu nabywania rulonów pikomonet i modułu płatności zainstalowanych na wielu różnych urządzeniach, takich jak smartfony, inteligentne telewizory, urządzenia automatyki domowej, samochody itp. Nie jest wymagane, aby oba moduły były zainstalowane na tym samym urządzeniu. Na przykład płatnik może użyć smartfonu, aby pobrać rulon pikomonet, a następnie przenieść go przez Bluetooth do modułu płatności zainstalowanego w samochodzie lub telewizorze.

Moduł płatności może działać jako rozszerzenie oprogramowania, które umożliwia korzystanie z określonej usługi. Na przykład moduł płatności może rozszerzyć odtwarzacz wideo na żądanie (VOD) zainstalowany w inteligentnym telewizorze, aby płacić strumieniowo za każdą sekundę oglądanego filmu.

Niskie koszty strumienia pikopłatności

System AMFI został zaprojektowany w taki sposób, aby koszty mocy obliczeniowej, transmisji i przechowywania danych wymaganych podczas strumienia pikopłatności były niskie. Podczas strumienia pikopłatności płatnik wysyła tylko identyfikatory kolejnych pikomonet, a odbiorca sprawdza, czy identyfikator kolejnej otrzymanej pikomony jest właściwie powiązany z identyfikatorem poprzedniej.

Wymagania нефunkcjonalne systemu AMFI

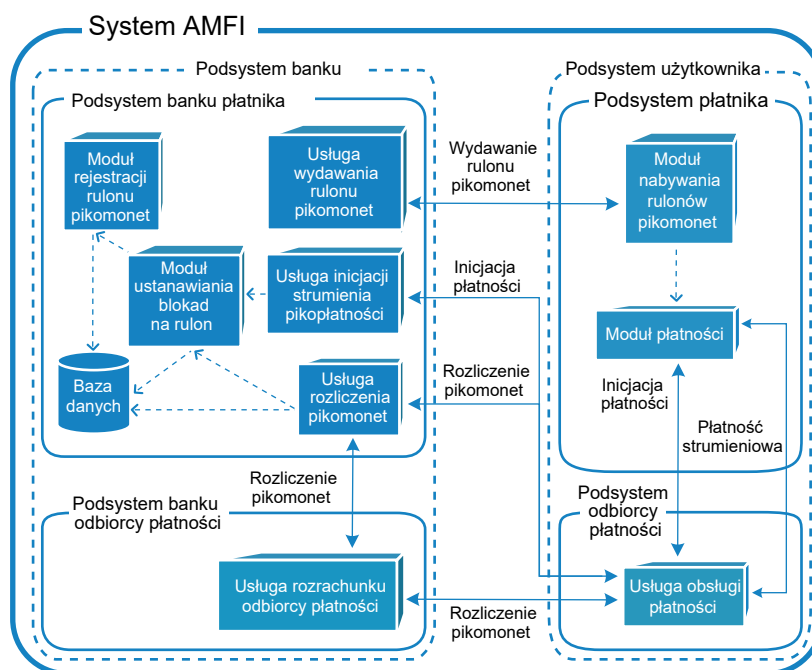
- 1) Wymiana danych w protokołach AMFI powinna być realizowana za pomocą bezpiecznych kanałów komunikacji, takich jak Secure Socket Layer (SSL) lub Transport Layer Security (TLS).



- 2) Urządzenia wykorzystywane przez system powinny być odpowiednio zabezpieczone przed nieuprawnionym dostępem (fizycznym lub programowym).
- 3) Implementacje zewnętrznych algorytmów wykorzystywanych w AMFI powinny być bezpieczne i nie wprowadzać podatności systemu na ataki.
- 4) Wszystkie podmioty działające w ramach systemu AMFI powinny przechowywać w tajemnicy wszystkie dane wpływające na bezpieczeństwo systemu m.in. klucze prywatne, identyfikatory niewykorzystanych pikomonet itp.
- 5) Każdy płatnik powinien mieć zawartą umowę z bankiem na korzystanie z pikopłatności strumieniowych – zgodnie z Art. 59k Ustawy o usługach płatniczych [Ustawa 2020/794].
- 6) Zakłada się, że każdy odbiorca płatności ma zawartą umowę z bankiem odbiorcy płatności pozwalającą na akceptowanie pikopłatności strumieniowych w systemie AMFI.

Komponenty systemu AMFI

Ze względu na pełnioną rolę podmiot systemu AMFI korzysta z odpowiedniego podsystemu, który składa się z modułów lub usług. Podsystemy składające się na system AMFI ilustruje Rysunek 3, a ich lista została zamieszczona poniżej.



Rysunek 3. Architektura komponentów systemu AMFI

A. Podsystem banku

1. Podsystem banku płatnika, w którego skład wchodzi:
 - 1.1. Usługa wydawania rulonu pikomonet
 - 1.2. Usługa inicjacji strumienia pikopłatności
 - 1.3. Usługa rozliczenia pikomonet
 - 1.4. Moduł rejestracji rulonu pikomonet
 - 1.5. Moduł ustanawiania blokad na rulon pikomonet

2. Podsystem banku odbiorcy, w którego skład wchodzi:

- 2.1. Usługa rozrachunku płatności

B. Podsystem użytkownika

1. Podsystem płatnika, w którego skład wchodzi:

- 1.1. Moduł nabywania rulonów pikomonet
- 1.2. Moduł płatności

2. Podsystem odbiorcy płatności

- 2.1. Usługa obsługi płatności



Techniczna realizacja systemu AMFI





6.1. Założenia wstępne

Płatności automatyczne rządzą się nieco odmiennymi prawami niż płatności dokonywane bezpośrednio przez ludzi. W przypadku tych ostatnich nie zwracamy większej uwagi na przykład na identyfikację punktu wnoszenia opłat (np. kasy fiskalnej), a także mamy pełną kontrolę nad całością procesu zapłaty, od podjęcia decyzji o zakupie, po moment autoryzacji środka płatniczego (np. karty bankowej). W zakupach kierujemy się zaufaniem do sklepu, ale jest to zaufanie określane raczej na drodze intuicyjnej („to miejsce wygląda dobrze, tu zrobimy dziś zakupy”, „ten hot-dog pachnie znakomicie, kupię go” itp.) niż formalnej – nikt z klientów raczej nie poprosi sprzedawcy o okazanie dowodu osobistego lub karty działalności gospodarczej.

Dokładnie odwrotna sytuacja występuje w przypadku realizacji płatności automatycznych. Nie ma tam miejsca na intuicję, a decyzję należy podjąć na podstawie „twardych” danych pozyskanych z zaufanych źródeł. Do tych danych należy zaliczyć:

- 1) *unikalny identyfikator* miejsca wnoszenia opłaty lub związanej z tym miejscem usługi; identyfikator ten musi być pozyskany na drodze zaufanej, uniemożliwiającej oszustwa, np. podszywanie się jednej usługi pod inną lub fałszowanie danych operatora usługi i odbiorcy płatności;
- 2) *zaufany typ usługi*, dostępny w ramach ogólnej klasyfikacji usług;
- 3) *zaufaną transmisję radiową* bliskiej odległości, w wersji minimalnej umożliwiającą tylko pobranie identyfikatora miejsca, w wersji pełnej – służącą także do wnoszenia opłaty i przesłania niezbędnych potwierdzeń.

Pierwszą i najważniejszą daną jest unikalny identyfikator. Dana ta musi być zaufana, czyli odpowiednio zaszyfrowana. Szyfrowanie musi uwzględniać zmienność kodu wynikowego w czasie, w celu uniemożliwienia ataku typu „nagraj i odtwórz”. Zaszyfrowany identyfikator musi mieć zatem ograniczony czas życia (na przykład minuta), aby zapobiec oszustwom, i być dostępny tylko w miejscu świadczenia usługi. Do celów rozgłaszania identyfikatora można wykorzystać:

- 1) *zmiennokodowe boje lokalizacyjne* Bluetooth Low Energy, rozgłaszające w tzw. kanale marketingowym BLE identyfikator wraz ze znacznikiem czasu, zaszyfrowane kluczem prywatnym;

- 2) ekran LCD/OLED z wyświetlanym kodem QR, zaszyfrowanym na tej samej zasadzie, co sygnał boi;
- 3) znacznik NFC o zmiennym kodzie (j.w.),
- 4) dane o aktualnej pozycji geograficznej, uzyskane z lokalizatora GPS.

W każdym z powyższych przypadków, za dynamiczne szyfrowanie identyfikatora odpowiada samo urządzenie, odpowiednio programując moduł boi, wyświetlacza, emulatora NFC lub nasłuchu zmian geolokalizacji.

Identyfikator każdego urządzenia jest zarejestrowany w ogólnodostępnej bazie danych, wraz z kluczem publicznym do odszyfrowania. Baza ta może być zdalnie dostępna z poziomu aplikacji płatnika lub jej fragmenty (głównie certyfikaty urządzeń z ich kluczami publicznymi) mogą być skopiowane do aplikacji. Dane te mogą być okresowo w niej uaktualniane, na tej samej zasadzie, jak programy antywirusowe aktualizują listę wirusów i innych możliwych ataków. Baza danych zawiera także informacje o typie usługi, w ramach ogólnej klasyfikacji wszystkich usług objętych systemem AMFI. Płatnik może wstępnie ustawić automatyczną realizację opłat tylko w stosunku do tych typów, którym ufa (np. opłat za miejski parking lub komunikację publiczną). Jeśli w zasięgu pojawi się usługa o typie niezaufanym, aplikacja może podjąć decyzję o jej odrzuceniu lub powiadomić płatnika o jej wykryciu, prosząc go o decyzję: zaakceptować na zawsze, odrzucić na zawsze lub zaakceptować na próbę (jednorazowo) w celu przetestowania, a potem ponowić prośbę o dokonanie klasyfikacji. W ten sposób każdy płatnik stopniowo tworzy listę typów usług, którym ufa, i w ramach których jego smartfon będzie dokonywać płatności automatycznie.

Ważną kwestią jest też wybór sieci lokalnej do komunikacji z urządzeniami, na rzecz których będą wnoszone opłaty. Choć w teorii może to być każda sieć oferująca szyfrowane i bezpieczne połączenie, w praktyce większość rozwiązań będzie się opierać na transmisji BLE, dla której naturalnym przedłużeniem jest komunikacja BLE Mesh. Sieć BLE Mesh jest siecią w pełni szyfrowaną i zaufaną, dodatkowo, ze względu na lokalność, utrudniającą śledzenie aktywności płatnika. Należy jednak dopuścić także możliwość zdalnej autoryzacji płatności – tutaj najlepszym kandydatem do zapewnienia łączności będzie standard LTE lub aktualnie wdrażana sieć 5G, na ogólnych zasadach bezpiecznej transmisji internetowej (czyli protokół SSL z listą zaufanych certyfikatów najwyższego poziomu oraz certyfikaty PKI).

6.2. Pobór opłat i świadczenie usługi lokalnie

W nawiązaniu do powyższej dyskusji, zakładamy, że w każdym miejscu opłat strumieniowych działa urządzenie, które:

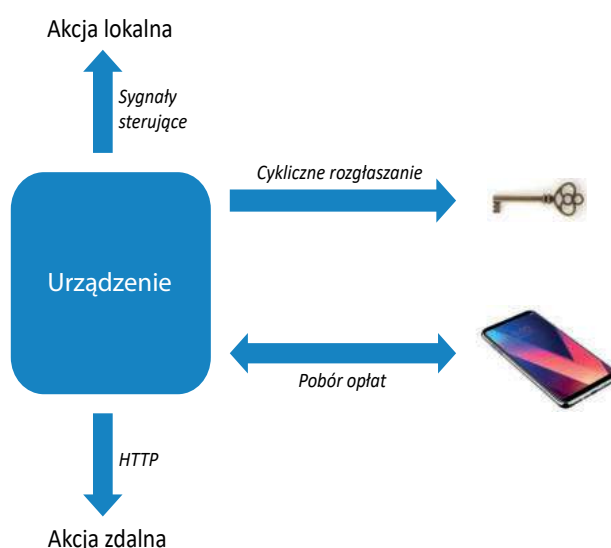
- 1) jest w stanie periodycznie rozgłaszać swój unikalny i zaufany identyfikator (klucz dostępowy), za pomocą transmisji radiowej lub optycznej bliskiego zasięgu,
- 2) jest w stanie wykonać pewną operację albo lokalnie (bez pośrednictwa sieci rozległej, na przykład podnieść/opuścić szlaban lub włączyć/wyłączyć ładowarkę indukcyjną), albo w kontakcie z określonym serwerem (na przykład poinformować o wejściu do pomieszczenia),
- 3) opcjonalnie jest w stanie przyjmować płatności strumieniowe za pomocą transmisji w sieci lokalnej (Rysunek 4).

W podstawowym trybie urządzenie rozgłasza swój identyfikator za pośrednictwem sieci radiowej (co pozwala na dostęp całkowicie automatyczny) bliskiego zasięgu – preferowaną siecią jest Bluetooth Low Energy (BLE) i kanał marketingowy (ang. Marketing Channel, MC), który umożliwia rozsyłanie komunikatów o maksymalnej długości 31 bajtów (pomijając dane kontrolne i sterujące). Identyfikator jest kodowany i zmieniany co określony czas (rzędu minut) na podobnej zasadzie, na jakiej działają generatory żetonów (ang. tokenizers) lub przy wykorzystaniu znacznika czasu (ang. time tag). Identyfikator jest pobierany za pośrednictwem aplikacji działającej w tle na smartfonie klienta (płatnika). Aplikacja dokonuje

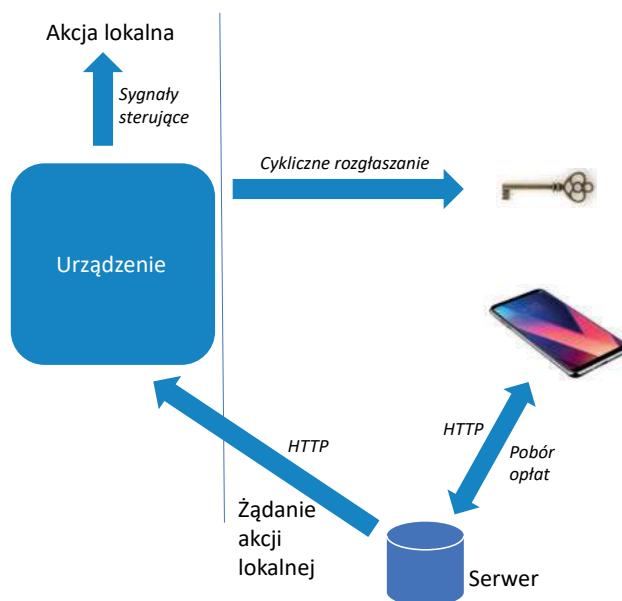
deszyfracji i tym samym weryfikacji poprawności (poziomu zaufania) do tej danej albo za pomocą wbudowanej bazy kluczy publicznych najwyższego rzędu, albo kontaktując się z wybranym serwerem i dokonując takiej weryfikacji zdalnie. Zweryfikowany i tym samym zaufany identyfikator staje się głównym wskazaniem na punkt poboru opłat, a także pośrednio – na odbiorcę płatności. Postać zaszyfrowana identyfikatora jest niepowtarzalna – ta właściwość uniemożliwia nagranie transmisji BLE/MC i odtworzenie jej w innym miejscu przez nieuprawnione osoby.

Smartfon, posiadając identyfikator, może go wykorzystywać do określenia kluczy dostępowych do sieci Bluetooth Mesh (BM). Klucze takie albo są pamiętane w aplikacji (i periodycznie uaktualniane po kontakcie z serwerem), albo on-line pobierane z serwera. Mając klucz, smartfon może nawiązać połączenie BM z urządzeniem i rozpocząć realizację protokołów dokonywania płatności.

Urządzenie, po nawiązaniu połączenia ze smartfonem, zaczyna udostępniać lokalnie usługę (np. włącza ładowarkę indukcyjną) i cyklicznie przesyła do smartfonu, kanałem BM, żądania zapłaty za czas świadczenia usługi, tworząc tym samym strumień pikopłatności. Świadczenie usługi kończy się w momencie, gdy smartfon przerwie połączenie BM – czyli gdy znajdzie się poza zasięgiem sieci radiowej (sytuacja typowa – klient wychodzi z zakresu świadczenia usługi, np. odjeżdża samochodem zaparkowanym nad ładowarką indukcyjną), albo gdy jego właściciel zdecyduje o zakończeniu współpracy (ręcznie przerywając połączenie). Może także wystąpić sytuacja awaryjna typu brak energii w baterii smartfonu i jego wyłączenie – jest to traktowane tak samo, jak pierwszy z opisanych powyżej przypadków.



Rysunek 4. Wymiana danych z urządzeniem świadczącym usługę



Rysunek 5. Wymiana danych z urządzeniem świadczącym usługę za pośrednictwem sieci rozległej

Urządzenie może świadczyć usługę lokalnie lub zdalnie. W pierwszym przypadku, jest ono wyposażone w stosowny mikrosterownik i moduł wykonawczy, np. stycznik włączający zasilanie ładowarki indukcyjnej. Polecenia do tego mikrosterownika są wydawane bezpośrednio w urządzeniu, które posiada stosowne oprogramowanie i linie wejścia/wyjścia. W drugim przypadku, urządzenie przez sieć rozległą (WiFi, LTE, 5G itp.) kontaktuje się z serwerem i informuje o każdej poprawnej płatności. Serwer jest odpowiedzialny za świadczenie usługi, która nie wymaga wykonania lokalnej akcji, ewentualnie wymaga programowego potwierdzenia dokonania zapłaty. Na przykład w ten sposób mogą być pobierane opłaty za przejazd komunikacją miejską – właściciel smartfonu cyklicznie płaci za przejazd, jednocześnie w każdej chwili może przedstawić kontrolerowi dowód takiej opłaty. Taki dowód także może być przesyłany w sieci lokalnej BM, co pozwala na automatyzację kontroli (kontroler podchodzi tylko do tych osób, których smartfony nie udowodniły zapłaty, przysyłając stosowne informacje, np. w sieci BLE Mesh lub przez kanał marketingowy BLE).

6.3. Pobór opłat i świadczenie usługi zdalnie

W drugim przypadku zakładamy, że smartfon nie jest cały czas dostępny w sieci lokalnej w miejscu świadczenia usługi. Dla przykładu, kierowca samochodu zostawia go na parkingu i idzie zrobić zakupy w pobliskim sklepie, wychodząc z zasięgu sieci BM urządzenia. W takim przypadku pobór opłat odbywa

się za pośrednictwem sieci rozległej i serwera (Rysunek 5). Po znalezieniu się w miejscu świadczenia usługi smartfon wykrywa i deszyfruje identyfikator tego miejsca. Jednak zamiast nawiązywać połączenie w sieci BM, smartfon przesyła ten identyfikator do serwera, za pomocą dowolnej sieci rozległej, do której ma akurat dostęp (zwykle będzie to transmisja LTE lub 5G). Adres serwera jest określany na podstawie identyfikatora na tej samej zasadzie, jak klucz dostępowy do sieci BM w pierwszym przypadku. Serwer jest odpowiedzialny za pobór opłat oraz ewentualny kontakt z urządzeniem, jeśli to urządzenie ma wykonać jakąś lokalną akcję (np. otworzyć szlaban lub uruchomić ładowarkę). Kontakt ten jest także realizowany za pomocą sieci rozległej (LTE/5G, ewentualnie dodatkowo WiFi jako technologia ostatniego metra).

6.4. Modyfikacje rozgłaszania identyfikatora

Wspomniany w poprzednich punktach zaszyfrowany identyfikator miejsca można rozgłaszać na kilka sposobów, niekoniecznie korzystając z transmisji radiowej MC/BLE. Kanałami takimi mogą być:

- 1) znacznik NFC (wymaga jednorazowego przybliżenia smartfonu do znacznika po przybyciu na miejsce świadczenia usługi, jest zatem trybem półautomatycznym),
- 2) kod QR (jw., dodatkowo wymaga ręcznego uruchomienia aplikacji do zrobienia zdjęcia tego kodu),

- 3) lokalizacja GPS – aplikacja może wykrywać miejsca świadczenia usług na podstawie danych o aktualnym położeniu smartfonu oraz parametrów jego ruchu (trzymany w ręce, uaktywniony/zablokowany, włączony w sieć pokładową samochodu itp. – dane z czujników telefonu pozwalają określić kontekst wykorzystania i chęci skorzystania z usługi).

W pierwszych dwóch przypadkach nie można skorzystać ze statycznych kodów, gdyż te mogą być łatwo skopiowane i wykorzystane w innym miejscu przez nieuprawnione osoby. Dlatego kody te muszą być zmienne w czasie, podobnie jak identyfikator przesyłany w sieci BLE/MC. W przypadku znacznika NFC musi to być moduł aktywny, który na polecenie z urządzenia zmienia cyklicznie zawartość informacyjną (może tym kanałem być nadawana dokładnie taka sama informacja, jak w kanale BLE/MC). W przypadku kodu QR nie może on być wydrukowany i nalepiony, a musi być wyświetlany na ekranie urządzenia (np. na ekranie zwyczajowo służącym do kontaktu z urządzeniem). Informacyjna zawartość tego kodu może być tożsama z informacjami przekazywanymi w sieci BLE/MC i NFC.

Należy także zauważyć, że lokalizacja GPS pozwala w pewnych przypadkach na całkowitą eliminację urządzenia pobierania opłat strumieniowych – realizacja płatności odbywa się w takim przypadku wyłącznie za pośrednictwem smartfonu i serwera, po znalezieniu się w danym miejscu i wykryciu tego faktu przez smartfon.

6.5. Kwestie implementacyjne

Zasięg rozsyłania identyfikatora w sieci BLE/MC można zmieniać programowo, ustalając siłę nadawania. W skrajnych przypadkach można ten zasięg poszerzyć do ok. 100 metrów w otwartym terenie lub zmniejszyć do kilkudziesięciu centymetrów (zakładając, że odbiorcą sygnału jest typowy smartfon). Zatem w zależności od potrzeb, można ograniczyć miejsce świadczenia usługi. Także pewne uwarunkowania zewnętrzne mogą mieć na to wpływ – na przykład nadajnik BLE/MC umieszczony wewnątrz metalowego tramwaju z zasięgiem ograniczonym do kilku metrów nie będzie radiowo widoczny na przystanku, przy którym pojazd się zatrzyma, także dlatego, że pojazd jest klatką Faradaya, blokującą fale elektromagnetyczne. W skrajnych przypadkach można skorzystać z kodów NFC lub QR, które są dostępne z odległości kilku (NFC) lub kilkudziesięciu (QR) centymetrów, choć to wymusza półautomatyzm rozwiązania.

Większość telefonów jest wyposażona w moduł BT/BLE, choć nie wszyscy użytkownicy telefonów mają ten moduł cały czas włączony na ciągle nasłuch sygnałów w paśmie BLE/MC, głównie ze względu na większe zużycie energii. W nowszych modelach telefonów taki

narzut energetyczny nie będzie przekraczać 20-25%, co oznacza ładowanie np. nie co trzy, a raz na dwa dni. Niektóre starsze modele telefonów (np. rozwiązania z systemami Android 5-7) mają ten narzut znacznie większy, dochodzący do 50%. Jednak na rynku i w użyciu jest ich coraz mniej, można się spodziewać, że w perspektywie dwóch - trzech lat praktycznie znikną.

Bardzo duża grupa użytkowników obawia się też utraty prywatności po odblokowaniu transmisji BT. Nie jest to słuszne podejście, w pewnym sensie jest to pozostałość po pierwszych generacjach Bluetooth (1.x i 2.x), które nie wykorzystywały szyfrowania transmisji i komunikowały swoją obecność każdemu w pobliżu. Sieć BLE Mesh jest w pełni zabezpieczona przed niepowołanym dostępem i możliwością podsłuchu, ze względu na wykorzystanie transmisji w pełni szyfrowanej. Świadomość tego faktu wśród użytkowników smartfonów ciągle rośnie i można się spodziewać, że w perspektywie kilku lat BT będzie powszechnie kojarzone z wysokim poziomem bezpieczeństwa.

Anonimowość systemu AMFI wiąże się z zastosowaniem specjalnej techniki kryptograficznej – tak zwanych ślepych podpisów (ang. blind signature). Oprogramowanie, które do tego służy, jak również modele matematyczne, na których to rozwiązanie zostało oparte, de facto nigdy nie zostały zastosowane w praktyce gospodarczej na większą skalę. Jest ryzyko, że ktoś w przyszłości odkryje słabości teoretyczne lub praktyczne tego rozwiązania (podobnie jak stopniowo odkrywano słabości technik kryptograficznych, które w konsekwencji były zastępowane innymi, doskonalszymi). Podobnie nie testowano na szerszą skalę technik kryptograficznych stosowanych w sieci BLE Mesh, która to sieć jest podstawą lokalnej transmisji danych w proponowanym rozwiązaniu. Z tego względu w rozwoju systemu należy uwzględnić monitoring zagrożeń w dziedzinie zaawansowanych technik kryptograficznych i odpowiednio szybko reagować na nowo pojawiające się niebezpieczeństwa.

W powyższym rozważaniu wskazujemy tylko na nowy sposób płatności, a nie kontroli dokonywania tych płatności. Opisywane urządzenia nie wyeliminują np. potrzeby kontroli zajęcia miejsc parkingowych lub biletów w tramwaju. Jednakże z drugiej strony za pomocą tej technologii można uniemożliwić korzystanie z pewnych usług – np. ładowarka indukcyjna, nawet jeśli połączenie będzie zestawione, nie uruchomi się bez zapłaty. Jednocześnie może ona wysłać stosowny komunikat do odpowiednich służb, które powinny w tradycyjny sposób zareagować i rozwiązać problem blokowania miejsca przez osobę/pojazd nieuprawniony. Nie zastąpi to kontroli przez człowieka, ale ułatwi i przyspieszy czynności, które muszą być wykonane przez nadzór.



Protokoły systemu AMFI

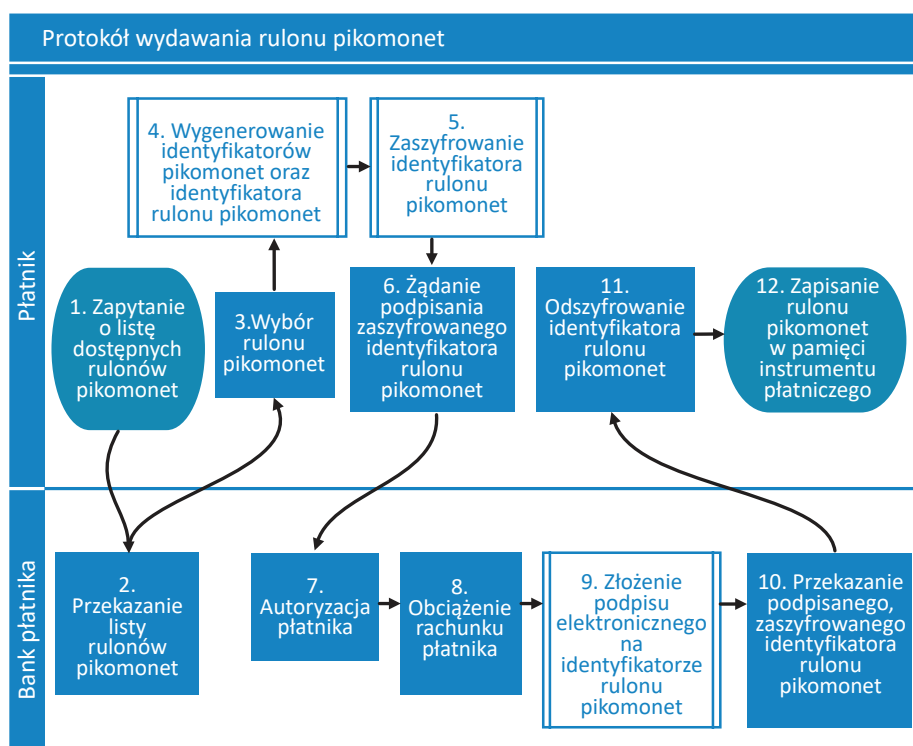


Funkcje systemu AMFI są realizowane za pomocą czterech protokołów: protokołu wydawania rulonu pikomonet, protokołu inicjowania płatności strumieniowej, protokołu przetwarzania transakcji płatniczych oraz protokołu wykupu pikomonet. Opis przebiegu tych protokołów jest opisany w kolejnych podrozdziałach.

7.1. Protokół wydawania rulonu pikomonet

Protokół wydawania rulonu pikomonet jest wykonywany między bankiem a płatnikiem za pośrednictwem internetu. Protokół ten pozwala płatnikowi na ustalenie nominałów pikomonet dostępnych w jego banku oraz uzyskanie rulonu pikomonet. Przebieg protokołu wydawania rulonu pikomonet ilustruje Rysunek 6, a jego opis został zamieszczony poniżej.

1. Płatnik wysyła do banku zapytanie o listę dostępnych rulonów pikomonet.
2. Bank płatnika udostępnia płatnikowi listę rulonów pikomonet, która dla każdego rulonu określa jego wartość oraz liczbę pikomonet wchodzących w jego skład (np. rulon o wartości 100 zł składa się ze stu tysięcy pikomonet o nominale 0,1 gr).
3. Płatnik wybiera rulon pikomonet, który chce zakupić od banku.
4. Płatnik wykonuje proces, który na podstawie losowej liczby wygeneruje identyfikatory pikomonet oraz identyfikator rulonu pikomonet.
5. Płatnik w celu anonimizacji rulonu pikomonet wykonuje proces szyfrowania identyfikatora rulonu pikomonet.
6. Płatnik wysyła do banku żądanie podpisania zaszyfrowanego identyfikatora rulonu pikomonet, które zawiera dane uwierzytelniające płatnika, zaszyfrowany identyfikator rulonu pikomonet oraz informacje o wartości i liczbie pikomonet w rulonie.
7. Bank płatnika autoryzuje żądanie płatnika po zwerifikowaniu jego danych uwierzytelniających.
8. Bank płatnika obciąża rachunek płatnika kwotą równą wartości żadanego rulonu pikomonet. W zależności od aktualnych regulacji prawnych, bank ma możliwość uwzględnienia w tym kroku protokołu opłaty za wydanie rulonu pikomonet.
9. Bank płatnika wykonuje proces, którego rezultatem jest podpis elektroniczny, złożony na zaszyfrowanym identyfikatorze rulonu pikomonet.
10. Bank płatnika przekazuje płatnikowi podpisany, zaszyfrowany identyfikator rulonu pikomonet.
11. Odszyfrowanie identyfikatora rulonu pikomonet
12. Zapisanie rulonu pikomonet w pamięci instrumentu płatniczego



Rysunek 6. Protokół wydawania rulonu pikomonet

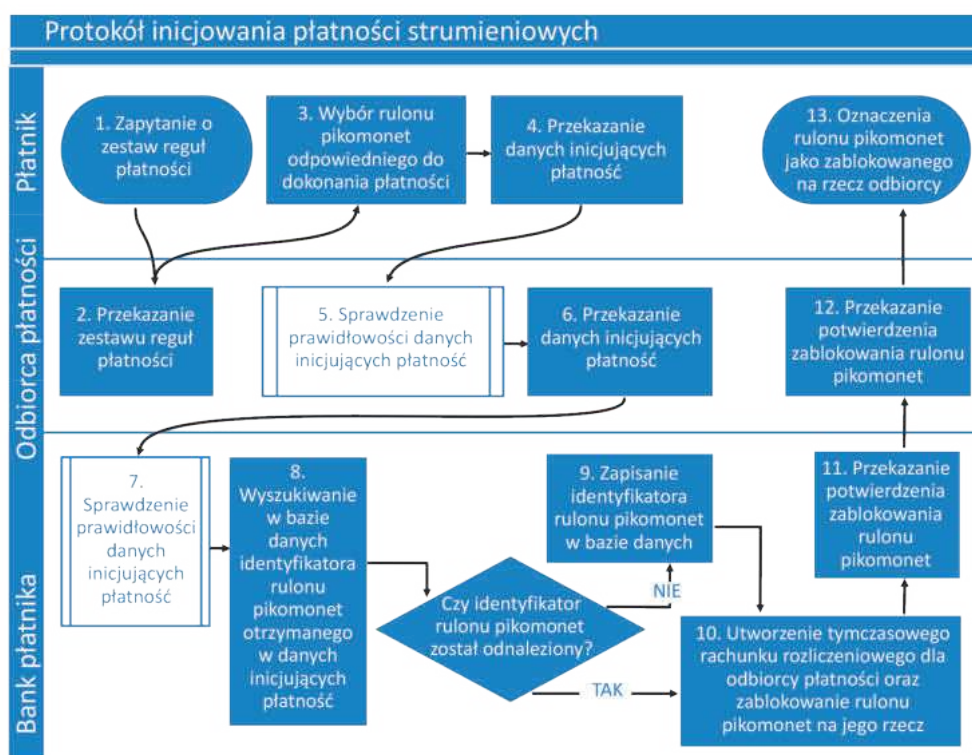
11. Płatnik odszyfrowuje podpisany, zaszyfrowany identyfikator rulonu pikomonet, na skutek czego pikomony stają się środkiem płatniczym.
12. Płatnik zapisuje rulon pikomonet w pamięci instrumentu płatniczego.

7.2. Protokół inicjowania płatności strumieniowej

Podczas realizacji protokołu inicjowania płatności strumieniowej, płatnik nawiązuje połączenie z odbiorcą płatności i przekazuje mu dane niezbędne do ustanowienia w banku płatnika blokady rulonu pikomonet na rzecz odbiorcy płatności. Techniczna realizacja połączenia z odbiorcą (WiFi, Bluetooth, NFC) nie ma znaczenia dla przebiegu protokołu i powinna być uwzględniona dopiero na etapie przygotowywania instrumentu płatniczego. Użyty do płatności rulon pikomonet czasowo zmienia swój stan z rulonu, którym można płacić dowolnemu odbiorcy płatności, na rulon dedykowany do płatności na rzecz określonego odbiorcy płatności. Powyższa metoda pozwala zapobiec wielokrotnemu użyciu tych samych pikomonet w kilku różnych płatnościach. Przebieg protokołu inicjowania płatności ilustruje Rysunek 7, a jego opis jest zamieszczony poniżej. Pozytywnie zakończony protokół inicjowania strumieniowej płatności umożliwia dokonywanie strumieniowych pikopłatności na

rzecz odbiorcy płatności przy wykorzystaniu rulonu pikomonet.

1. Płatnik wysyła do odbiorcy płatności zapytanie o zestaw reguł płatności związanych z usługą, za którą chce płacić.
2. Odbiorca płatności przekazuje płatnikowi zestaw reguł płatności. Zestaw reguł płatności jest dokumentem podpisanym elektronicznie przez odbiorcę płatności, który zawiera m.in. informacje o jednostce rozliczania usługi, cenie za jednostkę usługi, maksymalnym czasie blokady rulonu pikomonet oraz sposobie rozliczenia pikomonet przez odbiorcę.
3. Na podstawie danych zawartych w zestawie reguł płatności, płatnik (aplikacja płatnika) wybiera odpowiedni rulon pikomonet z dostępnych w instrumencie płatniczym.
4. Płatnik przekazuje odbiorcy płatności dane inicjujące płatność. Dane inicjujące płatność zawierają m.in. podpisany przez bank płatnika identyfikator rulonu pikomonet, wartość rulonu pikomonet, liczbę pikomonet w rulonie pikomonet, identyfikator ostatnio wydanej pikomony oraz numer porządkowy pikomony w rulonie pikomonet.
5. Odbiorca płatności sprawdza poprawność danych inicjujących płatność m.in. przez weryfikację

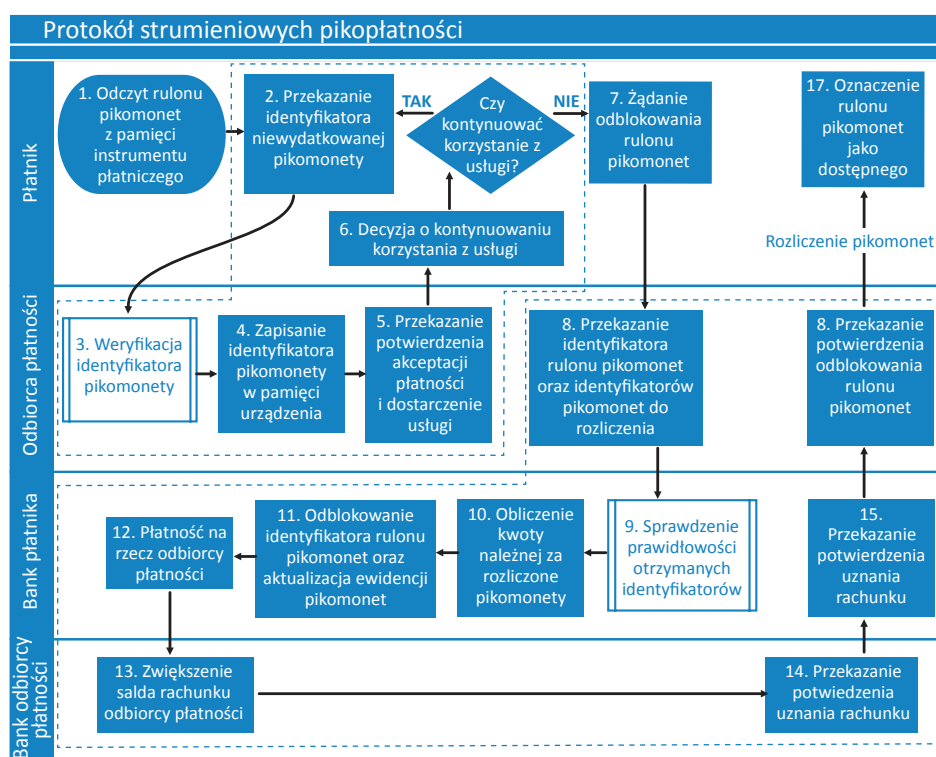


Rysunek 7. Protokół inicjowania płatności strumieniowych

- podpisu banku płatnika złożonego na identyfikatorze rulonu pikomonet oraz sprawdzenie powiązania między identyfikatorem rulonu pikomonet z ostatnio wydaną pikomonetą.
6. Po pozytywnej weryfikacji poprawności danych inicjujących płatność, odbiorca płatności łączy się z bankiem płatnika i przekazuje mu dane inicjujące płatność.
 7. Bank płatnika sprawdza poprawność danych inicjujących płatność, na wypadek, gdyby odbiorca płatności przesłał nieprawidłowe lub zmanipulowane dane.
 8. Po pozytywnej weryfikacji danych inicjujących płatność, bank płatnika wyszukuje w swojej bazie danych identyfikator rulonu pikomonet otrzymanego od odbiorcy płatności. Jeśli w bazie danych nie odnaleziono identyfikatora, bank przechodzi do realizacji kroku numer 9 protokołu, w przeciwnym przypadku, realizowany jest krok 10.
 9. Bank płatnika zapisuje identyfikator rulonu pikomonet w bazie danych w celu uniknięcia wielokrotnego wydania tych samych pikomonet. Z identyfikatorem rulonu pikomonet jest powiązana ewidencja pikomonet zużytych do płatności.
 10. Bank płatnika tworzy tymczasowy rachunek rozliczeniowy dla odbiorcy płatności oraz w celu uniknięcia wielokrotnego wydania tych samych pikomonet, blokuje rulon pikomonet na rzecz odbiorcy płatności do upływu czasu określonego w regułach płatności.
 11. Bank płatnika przekazuje odbiorcy płatności potwierdzenie zablokowania rulonu pikomonet na jego rzecz.
 12. Odbiorca płatności przekazuje potwierdzenie zablokowania rulonu pikomonet dalej do płatnika.
 13. Aplikacja płatnika oznacza rulon pikomonet zapisany w instrumencie płatniczym jako zablokowany na rzecz odbiorcy płatności.

7.3. Protokół strumieniowych pikopłatności

W przebieg protokołu strumieniowych pikopłatności są zaangażowani wszyscy aktorzy systemu. Protokół ten składa się z dwóch faz. Pierwsza faza to płatność strumieniowa, podczas której płatnik cyklicznie przekazuje odbiorcy płatności identyfikatory kolejnych pikomonet w zamian za jednostki usługi świadczonej na jego rzecz. Druga faza polega na rozliczeniu pikomonet, które następuje po zakończeniu świadczenia usługi. W wykonaniu protokołu strumieniowych



Rysunek 8. Protokół strumieniowych pikopłatności



pikopłatności uczestniczy czterech aktorów, przy czym w roli banku płatnika i banku odbiorcy płatności może występować ten sam podmiot, gdy zarówno płatnik, jak i odbiorca płatności korzystają z usług tego samego banku. Przebieg protokołu strumieniowych pikopłatności ilustruje Rysunek 8, a jego opis jest zamieszczony poniżej.

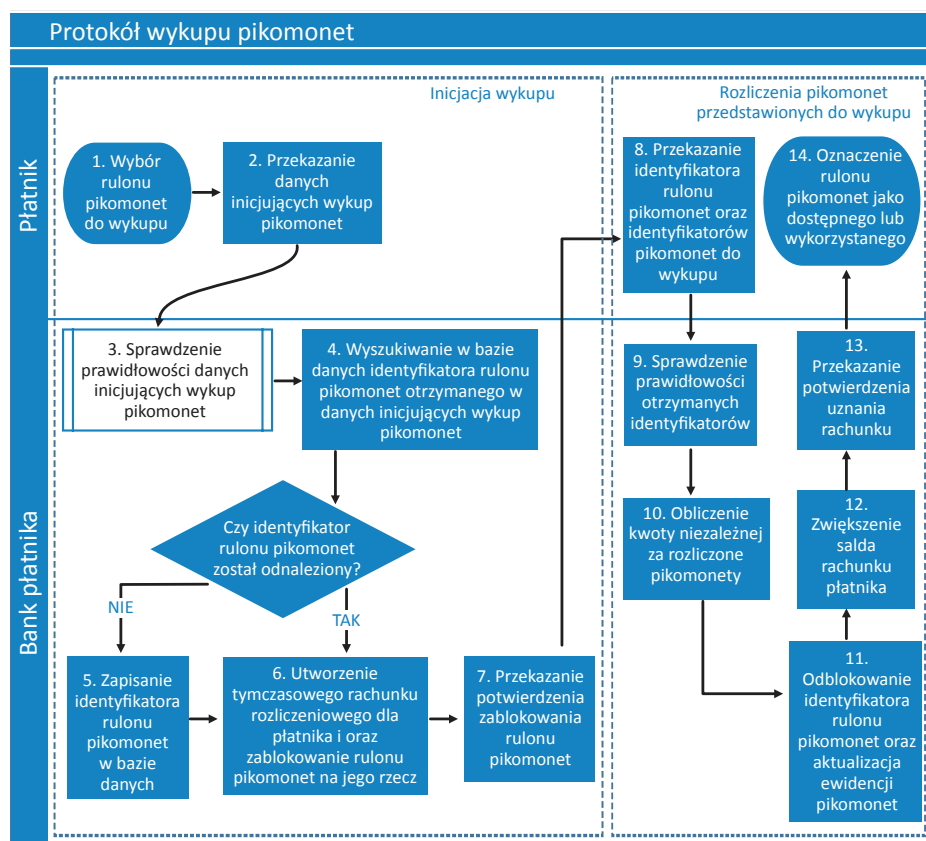
1. Płatnik odczytuje z pamięci instrumentu płatniczego dane o rulonie pikomonet, który został wybrany podczas protokołu inicjowania płatności strumieniowych, aby rozpocząć płatność strumieniową.
2. Płatnik wybiera identyfikator pikomonety, która reprezentuje jednostki pieniężne odpowiadające cenie usługi i przesyła go do odbiorcy płatności, aby skorzystać z usługi.
3. Odbiorca płatności weryfikuje pikomonetę sprawdzając, czy jest ona powiązana z identyfikatorem rulonu pikomonet oraz czy reprezentuje jednostki pieniężne odpowiadające cenie usługi.
4. Odbiorca płatności zapisuje identyfikator pikomonety w pamięci swojego urządzenia.
5. Odbiorca płatności przekazuje płatnikowi potwierdzenie akceptacji płatności oraz udostępnia usługę.
6. Płatnik decyduje, czy chce kontynuować korzystanie z usługi i płatności strumieniowej. Jeśli tak, to protokół przechodzi do kroku numer 2, w przeciwnym razie protokół przechodzi do kroku numer 7.
7. Płatnik przesyła do odbiorcy płatności żądanie odblokowania rulonu pikomonet, aby bank płatnika rozliczył wydane pikomonety i odblokował identyfikator rulonu pikomonet w swojej bazie danych.
8. Odbiorca płatności przekazuje do banku płatnika identyfikator rulonu pikomonet oraz identyfikator pikomonet w celu ich rozliczenia.
9. Bank płatnika sprawdza prawidłowość otrzymanych identyfikatorów rulonu pikomonet oraz pikomonet.
10. Na podstawie otrzymanych identyfikatorów bank płatnika oblicza kwotę płatności na rzecz odbiorcy płatności.
11. Bank płatnika odblokowuje identyfikator rulonu pikomonet oraz aktualizuje ewidencję pikomonet o identyfikatory rozliczonych pikomonet.

12. Bank płatnika dokonuje płatności na rzecz odbiorcy płatności przez wysłanie do banku odbiorcy płatności polecenia uznania jego rachunku.
13. Bank odbiorcy płatności zwiększa saldo rachunku odbiorcy płatności o kwotę wskazaną przez bank płatnika. W zależności od aktualnych regulacji prawnych, bank ma możliwość uwzględnienia w tym kroku protokołu opłaty za rozliczenie rulonu pikopłatności.
14. Bank odbiorcy płatności przesyła do banku płatnika potwierdzenie uznania konta odbiorcy płatności.
15. Bank płatnika przesyła potwierdzenie uznania konta odbiorcy płatności dalej do odbiorcy płatności.
16. Odbiorca płatności informuje płatnika o odblokowaniu przez bank płatnika rulonu pikomonet.
17. Płatnik oznacza rulon pikomonet jako dostępny i kończy wykonanie protokołu przetwarzania transakcji płatniczych.

W przypadku przerwania protokołu strumieniowych pikopłatności przez jedną ze stron lub z przyczyn leżących po stronie infrastruktury komunikacyjnej lub energetycznej, odbiorca płatności przed upływem czasu wygaśnięcia terminu blokady rulonu pikomonet u wydawcy przechodzi do punktu 8. protokołu, rozpoczynając fazę rozliczenia pikomonet.

7.4. Protokół wykupu pikomonet

W przebieg protokołu wykupu pikomonet są zaangażowani dwaj aktorzy systemu: płatnik i bank płatnika. Protokół ten składa się z dwóch faz. Pierwsza faza to inicjacja wykupu pikomonet – przebiega ona w sposób analogiczny do inicjacji płatności strumieniowej. Druga faza – rozliczenie pikomonet przedstawionych do wykupu – przebiega analogicznie do fazy rozliczenia pikomonet protokołu strumieniowych pikopłatności. Wykorzystanie procesów realizowanych we wcześniejszych protokołach pozwala na uproszczenie systemu, do tego stopnia, że bank realizuje wykup pikomonet, w taki sam sposób jak rozlicza pikomonety otrzymane od odbiorcy płatności. Powyższe rozwiązanie pozwala zapewnić anonimowość płatnika, gdyż bank nie wie, czy płatnik przedstawia do wykupu swoje pikomonety, czy rozlicza pikomonety otrzymane jako zapłatę od innego płatnika. Przebieg protokołu wykupu pikomonet ilustruje Rysunek 9, a jego opis jest zamieszczony poniżej.



Rysunek 9. Protokół wykupu pikomonet

1. Płatnik wybiera rulon pikomonet, którego pikomony chce przedstawić do wykupu. Płatnik może przedstawić do wykupu część niewydatkowanych pikomonet lub wszystkie pikomony wchodzące w skład rulonu pikomonet.
2. Płatnik przekazuje do banku płatnika dane inicjujące płatność. Dane inicjujące płatność zawierają m.in. podpisany przez bank płatnika identyfikator rulonu pikomonet, wartość rulonu pikomonet, liczbę pikomonet w rulonie pikomonet, identyfikator ostatnio wydanej pikomony, numer porządkowy pikomony w rulonie pikomonet oraz reguły płatności.
3. Bank płatnika sprawdza poprawność danych inicjujących płatność m.in. przez weryfikację swojego podpisu złożonego na identyfikatorze rulonu pikomonet oraz sprawdzenie powiązania między identyfikatorem rulonu pikomonet z ostatnio wydaną pikomonetą.
4. Po pozytywnej weryfikacji danych inicjujących płatność, bank płatnika wyszukuje w swojej bazie danych identyfikator rulonu pikomonet otrzymanego od odbiorcy płatności. Jeśli w bazie danych nie odnaleziono identyfikatora, bank przechodzi do realizacji kroku numer 5 protokołu, w przeciwnym przypadku, realizowany jest krok 6.
5. Bank płatnika zapisuje identyfikator rulonu pikomonet w bazie danych w celu uniknięcia wielokrotnego wydania tych samych pikomonet. Z identyfikatorem rulonu pikomonet jest powiązana ewidencja pikomonet użytych do płatności.
6. Bank płatnika tworzy tymczasowy rachunek rozliczeniowy dla płatnika oraz, w celu uniknięcia wielokrotnego wydania tych samych pikomonet, blokuje rulon pikomonet na rzecz płatnika do upływu czasu określonego w regułach płatności.
7. Bank płatnika przekazuje płatnikowi potwierdzenie zablokowania rulonu pikomonet na jego rzecz.
8. Płatnik przekazuje do banku płatnika identyfikator rulonu pikomonet oraz identyfikatory pikomonet w celu ich wykupu.
9. Bank płatnika sprawdza prawidłowość otrzymanych identyfikatorów rulonu pikomonet oraz pikomonet.
10. Na podstawie otrzymanych identyfikatorów, bank płatnika oblicza kwotę płatności na rzecz płatnika.

11. Bank płatnika odblokowuje identyfikator rulonu pikomonet oraz aktualizuje ewidencję pikomonet o identyfikatory wykupionych pikomonet.
12. Bank płatnika zwiększa saldo rachunku płatnika o kwotę płatności. W zależności od aktualnych regulacji prawnych, bank ma możliwość uwzględnienia w tym kroku protokołu opłaty za wykup rulonu pikomonet.
13. Bank płatnika przesyła do płatnika potwierdzenie uznania jego konta.
14. Płatnik oznacza rulon pikomonet jako dostępny lub wykorzystany i kończy wykonanie protokołu wykupu pikomonet.

7.5. Proponowany interfejs programowy dla celów komunikacji płatników z bankiem rozliczającym pikomonety

Interfejs umożliwiający komunikację płatnika z bankiem (Rysunek 10) jest wykorzystywany w systemie AMFI w celu wydawania rulonu pikomonet. Bank udostępnia płatnikom w internecie usługę sieciową (usługa wydawania rulonu pikomonet) realizowaną przy wykorzystaniu protokołu HTTPS oraz architektury REST. Komunikaty są wymieniane w postaci dokumentów w formacie JSON. Płatnik, korzystając z dedykowanego oprogramowania zainstalowanego na swoim urządzeniu (modułu nabywania rulonu pikomonet), wywołuje funkcje usługi udostępnionej przez bank.

Usługa wydawania pikomonet oferuje następujące funkcje:

- silne uwierzytelnienie płatnika,

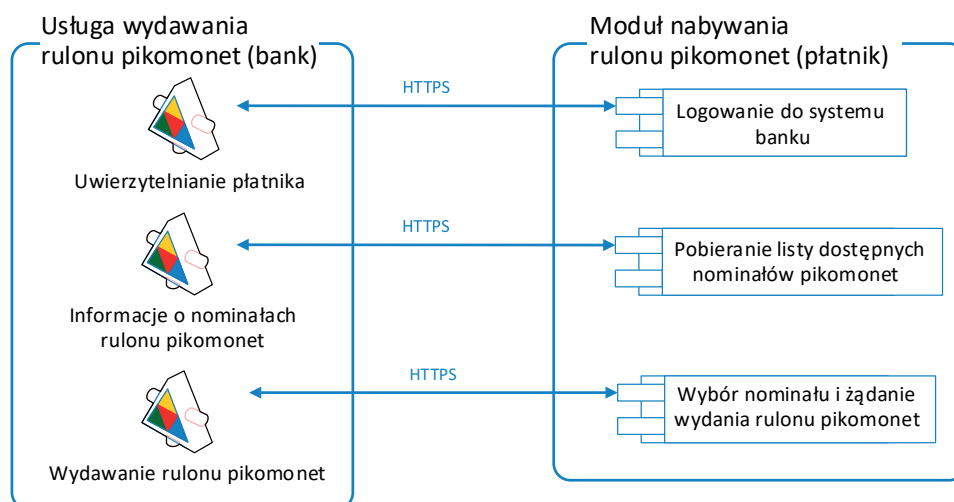
- informacje o dostępnych nominałach rulonów pikomonet,
- wydawanie rulonu pikomonet (pieniądza elektronicznego).

7.6. Proponowany interfejs programowy protokołu systemu pikopłatności w inteligentnym mieście na styku płatnik – usługodawca

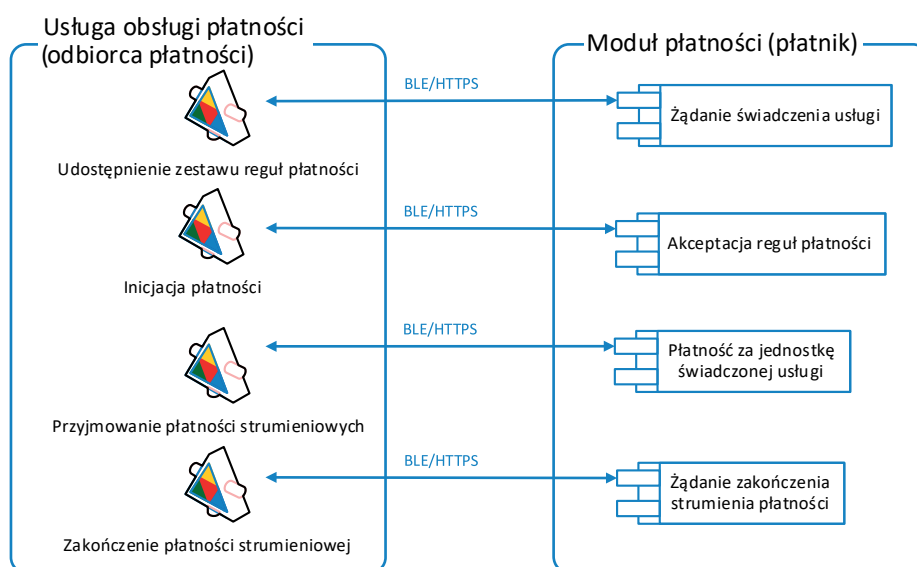
Interfejs umożliwiający komunikację płatnika z usługodawcą (Rysunek 11) jest wykorzystywany w systemie AMFI w celu inicjacji płatności oraz realizacji płatności strumieniowej. Usługodawca udostępnia płatnikom usługę obsługi płatności, która może być realizowana przy wykorzystaniu protokołów komunikacji na bliską odległość (np. Bluetooth Low Energy – BLE) lub przy wykorzystaniu protokołu HTTPS oraz architektury REST. Komunikaty są wymieniane w postaci dokumentów w formacie JSON. Płatnik, korzystając z dedykowanego oprogramowania zainstalowanego na swoim urządzeniu (modułu płatności), wywołuje funkcje usługi udostępnionej przez usługodawcę.

Usługa obsługi płatności oferuje następujące funkcje:

- negocjacja spełnienia wybranych i sparametryzowanych reguł i udostępnienie zestawu reguł płatności,
- inicjacja płatności,
- przyjmowanie płatności strumieniowych,
- zakończenie płatności strumieniowej.



Rysunek 10. Interfejs płatnik – bank



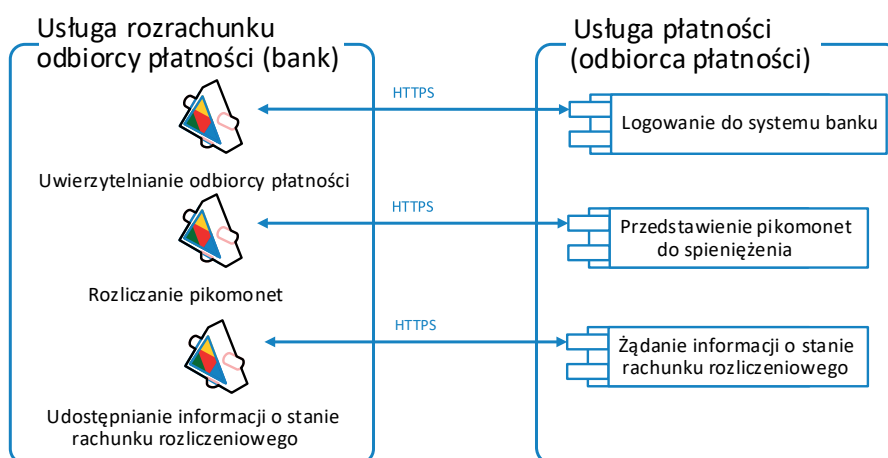
Rysunek 11. Interfejs płatnik – usługodawca

7.7. Proponowany interfejs programowy protokołu systemu pikopłatności w inteligentnym mieście na styku usługodawca – bank

Interfejs umożliwiający komunikację usługodawcy z bankiem (Rysunek 12) jest wykorzystywany w systemie AMFI w celu rozliczenia pikomonet. Bank udostępnia usługodawcy w internecie usługę sieciową (usługa rozrachunku odbiorcy płatności) realizowaną przy wykorzystaniu protokołu HTTPS oraz architektury REST. Komunikaty są wymieniane w postaci dokumentów

w formacie JSON. Usługodawca, korzystając z dedykowanego oprogramowania zainstalowanego na swoim urządzeniu (usługa płatności), wywołuje funkcje usługi udostępnionej przez bank. Usługa rozrachunku odbiorcy płatności oferuje następujące funkcje:

- silne uwierzytelnianie odbiorcy płatności,
- rozliczanie pikomonet,
- udostępnianie informacji o stanie rachunku rozliczeniowego.



Rysunek 12. Interfejs usługodawca – bank



System pikopłatności strumieniowych w świetle Ustawy o usługach płatniczych oraz rozporządzenia Komisji Europejskiej 2018/389



Celem tego rozdziału jest ocena zgodności architektury i protokołów AMFI z obowiązującymi w Polsce przepisami prawa. Ze względu na rozbudowane przepisy dotyczące usług płatniczych, brak prawnej definicji technicznych pojęć zawartych w Ustawie o usługach płatniczych oraz nieprecyzyjny charakter niektórych przepisów, przedstawione w tym rozdziale wnioski nie mają charakteru ekspertyzy prawnej, która jest niezbędna przed wdrożeniem systemu AMFI do praktyki gospodarczej.

Parlament Europejski i Rada mając na celu ciągły rozwój zintegrowanego rynku wewnętrznego bezpiecznych płatności elektronicznych oraz zapewnienie konsumentom, akceptantom i przedsiębiorstwom wyboru i przejrzystości usług płatniczych przyjęły w dniu 25 listopada 2015 r. Dyrektywę 2015/2366 w sprawie usług płatniczych w ramach rynku wewnętrznego (nazywaną skrótowo PSD2) [Dyrektywa 2015/2366]. Dyrektywa 2015/2366 zobowiązała państwa członkowskie Unii Europejskiej do transpozycji postanowień dyrektywy do dnia 13 stycznia 2018 r. Postanowienia powyższej dyrektywy zostały wprowadzone do polskiego porządku prawnego w drodze nowelizacji ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych Dz.U.2020.794 [Ustawa 2019/1781].

Mając na względzie bezpieczeństwo usług płatniczych oferowanych drogą elektroniczną, Komisja Europejska przyjęła Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji. Rozporządzenie to wiąże państwa członkowskie w całości i jest przez nie bezpośrednio stosowane.

Kolejne podrozdziały odnoszą rozwiązania zaproponowane w systemie AMFI do poszczególnych zapisów Ustawy o usługach płatniczych.

8.1. Konstrukcja systemu AMFI w kontekście definicji prawnych

System AMFI pozwala na transfer środków pieniężnych oparty na formalnych i znormalizowanych regulacjach opisanych w Rozdziale 7, co pozwala, na podstawie art. 2 pkt 27 Ustawy o usługach płatniczych, określić go jako system płatniczy.

Pikomony, zastosowane do realizacji transakcji płatniczych, stanowią wartość pieniężną przechowywaną elektronicznie w urządzeniu płatnika, która jest wydawana przez bank z obowiązkiem jej wykupu

i akceptowana przez odbiorców płatności będącymi innymi podmiotami niż bank, co pozwala, na podstawie art. 2 pkt 21a Ustawy o usługach płatniczych, uznać je za pieniądź elektroniczny.

Płatnik, w celu dokonania transakcji płatniczej, realizuje niezależny od urzędnika, uzgodniony zbiór procedur, co pozwala, na podstawie art. 2 pkt 10 Ustawy o usługach płatniczych, uznać protokoły systemu AMFI za instrument płatniczy – w systemie AMFI zrezygnowano z wykorzystania zindywidualizowanego urządzenia na rzecz uniwersalnych urządzeń osobistych płatnika (smartfon, tablet, laptop), co nie stoi w sprzeczności z Ustawą o usługach płatniczych.

Zastosowanie w systemie płatniczym pieniądza elektronicznego powoduje, że na podstawie art. 7 ust. 4 Ustawy o usługach płatniczych środki pieniężne otrzymywane w zamian za wydany pieniądź elektroniczny nie mogą być oprocentowane ani nie mogą przynosić posiadaczowi pieniądza elektronicznego żadnych innych pożytków uzależnionych od okresu posiadania pieniądza elektronicznego. Jednocześnie art. 7 ust. 1 Ustawy o usługach płatniczych nie odebrał bankom krajowym prawa do obracania środkami pieniężnymi, za które został wydany pieniądź elektroniczny [Bajor i inni 2017, Ustawa 2020/794]. Z powyższych przesłanek wynika, że bank może swobodnie obracać środkami otrzymanymi w zamian za wydany pieniądź elektroniczny i nawet nie tyle, że bez obowiązku, lecz wręcz w warunkach prawnego zakazu udzielania jakichkolwiek pożytków posiadaczowi pieniądza elektronicznego.

Nazwy uczestników systemu AMFI wprost odnoszą się do podmiotów i ról zdefiniowanych w Ustawie o usługach płatniczych. Definicja płatnika przytoczona w Rozdziale 2 wprost odpowiada definicji określonej w art. 2 pkt. 22 Ustawy o usługach płatniczych. Definicja odbiorcy płatności zastosowana w tym raporcie odpowiada definicji odbiorcy, określonej w art. 2 pkt. 18 Ustawy o usługach płatniczych. W systemie AMFI rolę wydawcy pieniądza elektronicznego pełni bank, co jest zgodne z art. 4 ust. 2b Ustawy o usługach płatniczych.

8.2. Silne uwierzytelnianie

W art. 32i Ustawy o usługach płatniczych ustawodawca wprowadził wymóg stosowania przez dostawcę silnego uwierzytelniania użytkownika w przypadkach, gdy płatnik uzyskuje dostęp do swojego rachunku w trybie online, inicjuje elektroniczną transakcję płatniczą oraz gdy przeprowadza za pomocą kanału zdalnego czynność, która może wiązać się z ryzykiem oszustwa związanego z wykonywanymi usługami

płatniczymi lub innych nadużyć. Ustawodawca w art. 2 pkt. 26aa Ustawy o usługach płatniczych zdefiniował silne uwierzytelnianie użytkownika jako uwierzytelnianie zapewniające ochronę poufności danych w oparciu o zastosowanie co najmniej dwóch metod należących do kategorii „wiedza o czymś”, o czym wie wyłącznie użytkownik, „posiadanie czegoś”, co posiada wyłącznie użytkownik lub cechy charakterystycznej użytkownika. Przy czym ustawodawca zastrzegł, że naruszenie jednej z tych metod uwierzytelniania nie osłabia wiarygodności pozostałych.

Uwierzytelnianie oznacza proces, w którym jeden podmiot poznaje tożsamość drugiego podmiotu, który jest zobowiązany do jej udowodnienia podczas wykonywania protokołu weryfikacji tożsamości [Zucherato 2011]. Wymóg uwierzytelniania użytkownika usług płatniczych w praktyce uniemożliwia mu korzystanie z nich w sposób anonimowy. Anonimowość w kontekście systemów informatycznych jest definiowana jako ochrona tożsamości użytkownika przez umożliwienie mu korzystania z zasobów lub usług bez ujawniania swojej tożsamości [CCITSE 2012].

W systemie AMFI bank stosuje silne uwierzytelnianie płatnika podczas wydawania rulonu pikomonet. Natomiast inicjacja oraz dokonywanie płatności pikomonetami następuje w drodze ujawniania i weryfikacji identyfikatorów pikomonet, które są przechowywane w urządzeniu płatnika. W przypadku stosowania silnego uwierzytelniania, automatyczne płatności strumieniowe byłyby niemożliwe do realizacji, gdyż dwie z trzech dopuszczalnych metod silnego uwierzytelniania wymagają wykonania czynności od użytkownika (np. wpisania numeru PIN, hasła, zeskanowania odcisku palca, wypowiedzenia frazy).

Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych, bezpiecznych i otwartych standardów komunikacji dopuszcza wyłączenia z obowiązku stosowania silnego uwierzytelniania klienta wobec specyficznych technologii płatności. Art. 11 Rozporządzenia 2018/389 wyłącza wymóg stosowania silnego uwierzytelniania w przypadku, gdy płatnik inicjuje zbliżeniową elektroniczną transakcję płatniczą i jeżeli spełnione zostały łącznie warunki dotyczące kwoty zbliżeniowej transakcji, która nie może przekroczyć 50 EUR oraz łącznej kwoty wcześniejszych zbliżeniowych elektronicznych transakcji płatniczych zainicjowanych za pomocą instrumentu płatniczego posiadającego funkcję płatności zbliżeniowej od dnia ostatniego zastosowania silnego uwierzytelnienia klienta, która nie może przekroczyć 150 EUR oraz

liczby następujących po sobie zbliżeniowych elektronicznych transakcji płatniczych zainicjowanych za pomocą instrumentu płatniczego posiadającego funkcję płatności zbliżeniowej od dnia ostatniego zastosowania silnego uwierzytelnienia klienta, która nie może przekroczyć pięciu.

Podobne wyłączenie wprowadza art. 16 Rozporządzenia 2018/389, który uchyła wymóg silnego uwierzytelniania w przypadku, gdy płatnik inicjuje zdalną elektroniczną transakcję płatniczą, dla której kwota zdalnej elektronicznej transakcji płatniczej nie przekracza 30 EUR oraz łączna kwota poprzednich zdalnych elektronicznych transakcji płatniczych zainicjowanych przez płatnika od dnia ostatniego zastosowania silnego uwierzytelnienia klienta nie przekracza 100 EUR oraz liczba poprzednio wykonanych zdalnych elektronicznych transakcji płatniczych zainicjowanych przez płatnika od dnia ostatniego zastosowania silnego uwierzytelnienia klienta nie przekracza pięciu następujących po sobie, pojedynczych zdalnych elektronicznych transakcji płatniczych.

Prawodawca Europejski w art. 12 Rozporządzenia 2018/389 wyłączył obowiązek stosowania silnego uwierzytelniania wobec terminali samoobsługowych służących uiszczaniu opłat za przejazd i opłat za postój. Art. 13 Rozporządzenia 2018/389 stanowi również, że dostawcy usług płatniczych mogą nie stosować silnego uwierzytelniania klienta, z zastrzeżeniem spełnienia ogólnych wymogów dotyczących uwierzytelniania, jeżeli płatnik inicjuje transakcję płatniczą, a odbiorca znajduje się na liście zaufanych odbiorców utworzonej uprzednio przez płatnika. W Rozporządzeniu 2018/389, w art. 18 również przewidziano wyłączenie obowiązku silnego uwierzytelniania płatnika, jeśli płatnik inicjuje zdalną elektroniczną transakcję płatniczą, którą dostawca usług płatniczych uzna za charakteryzującą się niskim poziomem ryzyka zgodnie z mechanizmami monitorowania transakcji przewidzianymi w tym rozporządzeniu. Mechanizm monitorowania transakcji stoi w sprzeczności z anonimowością płatnika, gdyż zgodnie z art. 18 ust. 2 pkt c wymaga m.in. ustalenia wzorca zachowań płatnika oraz jego lokalizacji.

Na podstawie literalnego brzmienia przepisów Rozporządzenia delegowanego Komisji (UE) 2018/389, system AMFI nie może skorzystać z możliwości uchylenia obowiązku stosowania silnego uwierzytelniania. Jednocześnie takie cechy systemu AMFI jak anonimowość płatnika oraz automatyczne płatności nie pozwalają na stosowanie silnego uwierzytelniania podczas inicjacji płatności oraz jej dokonywania. Ustawodawca Europejski nie dostosował przepisów do systemów płatności bazujących na pieniądzu elektronicznym w postaci produktu cyfrowego (nie

usługi), który z technicznego punktu widzenia, w przypadku AMFI ma postać jednorazowego, elektronicznego znaku pieniężnego. W systemie AMFI silne uwierzytelnianie użytkownika jest stosowane podczas realizacji protokołu wydawania rulonu pikomonet. Po uzyskaniu rulonu pikomonet, to w dużej mierze na użytkownika spoczywa odpowiedzialność za zapewnienie ich bezpieczeństwa, podobnie jak ma to miejsce w przypadku znaków pieniężnych.

8.3. Możliwość odstąpienia od niektórych regulacji prawnych w przypadku mikropłatności

W artykule 19 oraz 39 Ustawy o usługach płatniczych ustawodawca umożliwił dostawcy usługi płatniczej uzgodnienie z użytkownikiem w treści umowy ramowej wyłączenia określonych wybranych regulacji Ustawy o usługach płatniczych związanych z autoryzacją transakcji, możliwością jej odwołania lub chwili uznania rachunku płatniczego odbiorcy, po spełnieniu przez instrument płatniczy jednego z następujących wymogów [Bajor i inni 2017, Ustawa 2020/794]:

- kwota indywidualnej transakcji płatniczej nie przekracza równowartości 30 EUR lub nie przekracza 60 EUR w przypadku transakcji płatniczych wykonywanych w całości na terytorium Rzeczypospolitej Polskiej, lub nie przekracza 500 EUR w odniesieniu do przedpłaconych instrumentów płatniczych w przypadku transakcji płatniczych wykonywanych w całości na terytorium Rzeczypospolitej Polskiej,
- limit wydatków w wysokości 150 EUR lub w wysokości 300 EUR w przypadku transakcji płatniczych wykonywanych w całości na terytorium Rzeczypospolitej Polskiej lub w wysokości 500 EUR w odniesieniu do przedpłaconych instrumentów płatniczych w przypadku transakcji płatniczych,
- instrument płatniczy służy do przechowywania środków pieniężnych w kwocie nieprzekraczającej w żadnym momencie 150 EUR lub nieprzekraczającej 300 EUR w przypadku transakcji płatniczych wykonywanych w całości na terytorium Rzeczypospolitej Polskiej, lub nieprzekraczającej 500 EUR w odniesieniu do przedpłaconych instrumentów płatniczych w przypadku transakcji płatniczych.

W powyższych przypadkach dostawca usługi płatniczej może w umowie ramowej z użytkownikiem postanowić, że:

- płatnik nie może odwołać zlecenia płatniczego po przekazaniu odbiorcy zlecenia płatniczego lub udzieleniu odbiorcy swojej zgody na wykonanie transakcji

płatniczej (nie stosuje się art. 51 Ustawy o usługach płatniczych),

- dostawca nie ma obowiązku powiadomienia użytkownika o odmowie wykonania zlecenia płatniczego, jeżeli z okoliczności jasno wynika, iż zlecenie nie zostało wykonane (nie stosuje się art. 50 ust. 1-3 Ustawy o usługach płatniczych),
- nie mają zastosowania terminy uznania rachunku dostawcy odbiorcy kwotą transakcji płatniczej oraz udostępnienia odbiorcy kwoty transakcji przez dostawcę odbiorcy określone w art. 54, art. 56 i art. 57,
- nie ma zastosowania art. 29 (regulacje dotyczące zmian w postanowieniach umownych) oraz art. 26 ust. 1 zobowiązujący dostawcę do dostarczania użytkownikowi informacji w postaci papierowej lub na innym trwałym nośniku informacji,
- dostawca dostarcza płatnikowi jedynie informacje o głównych cechach usługi płatniczej oraz inne podstawowe informacje o możliwych sposobach korzystania z instrumentu płatniczego, zakresie odpowiedzialności ponoszonej za wykonanie usługi przez dostawcę, pobieranych opłatach, miejscu uzyskania dostępu do informacji wymienionych w art. 27,
- dostawca dostarcza lub udostępnia użytkownikowi jedynie informacje umożliwiające zidentyfikowanie transakcji płatniczej i jej kwoty oraz pobranych opłat, a w przypadku kilku transakcji płatniczych tego samego rodzaju i na rzecz tego samego odbiorcy - informacje o całkowitej kwocie tych transakcji płatniczych i opłatach pobranych z ich tytułu,
- dostawca nie ma obowiązku dostarczania lub udostępniania informacji wymienionych w poprzednim punkcie, jeżeli instrument płatniczy używany jest anonimowo lub jeżeli z innych względów dostawca nie ma technicznej możliwości ich dostarczenia, jednak zobowiązany jest do zapewnienia płatnikowi możliwości sprawdzenia kwoty przechowywanych środków pieniężnych,
- jeżeli instrument płatniczy jest używany anonimowo lub dostawca z innych przyczyn nieodłącznie związanych z instrumentem płatniczym nie jest w stanie udowodnić, że transakcja była autoryzowana, nie stosuje się przepisów art. 45 (spoczywanie na dostawcy użytkownika ciężaru udowodnienia, że transakcja płatnicza została autoryzowana i prawidłowo zapisana w systemie służącym do obsługi transakcji płatniczych dostawcy oraz że nie miała na nią wpływu awaria techniczna ani innego rodzaju usterka związana z usługą płatniczą świadczoną przez tego dostawcę, w tym dostawcę świadczącego usługę



inicjowania transakcji płatniczej) oraz art. 46 ust. 1-3 (obowiązek zwrotu płatnikowi przez dostawcę kwoty nieautoryzowanej transakcji, kwotowy limit odpowiedzialności płatnika za nieautoryzowane transakcje płatnicze, braku limitu odpowiedzialności płatnika za nieautoryzowane transakcje płatnicze, jeśli płatnik doprowadził do nich umyślnie lub na skutek rażącego niedbalstwa),

- jeżeli instrument płatniczy nie pozwala na jego zablokowanie lub uniemożliwienie w inny sposób jego dalszego używania, nie stosuje się przepisów art. 42 ust. 1 pkt 2 (obowiązek niezwłocznego zgłoszenia dostawcy przez użytkownika utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu), art. 43 ust. 1 pkt 3-5 (zapewnienie przez dostawcę środków, procedur do dokonania zgłoszenia, o którym mowa w art. 42, uniemożliwienie korzystania z instrumentu po dokonaniu zgłoszenia oraz nienakładanie opłat w wysokości przekraczającej koszty bezpośrednio związane z wydaniem nowego instrumentu płatniczego w miejsce instrumentu, którego zgłoszenie na podstawie art. 42 dotyczy) i art. 46 ust. 4 i 5 (wyłączenie odpowiedzialności płatnika za nieautoryzowane transakcje płatnicze) Ustawy o usługach płatniczych.

System AMFI pozwala na wydawanie pieniędzy elektronicznego w postaci rulonów pieniądza elektronicznego o wartości określonej przez bank. Rozwiązanie to ogranicza maksymalną wartość pojedynczej transakcji płatniczej do wartości rulonu pikomonet (transakcja musi zostać rozliczona po wydaniu ostatniej pikomonety). Jeżeli bank będzie emitował pieniądź elektroniczny w rulonach o wartości odpowiadającej w walucie polskiej równowartości co najwyżej 30 EUR, spełni przesłanki umożliwiające wyłączenie w umowie ramowej z użytkownikiem niektórych przepisów Ustawy o usługach płatniczych.

System AMFI udostępnia płatnikowi instrument płatniczy zapewniający jego anonimowość, co spełnia przesłanki do wyłączenia w umowie ramowej z użytkownikiem niektórych przepisów Ustawy o usługach płatniczych.

W systemie AMFI rolę instrumentu płatniczego pełni urządzenie użytkownika oraz oprogramowanie, nad którym bank nie sprawuje kontroli oraz nie ma możliwości jego zablokowania, w związku z czym zachodzą przesłanki do wyłączenia w umowie ramowej z użytkownikiem przepisów zawartych w art. 42 ust. 1 pkt 2, art. 43 ust. 1 pkt 3-5 i art. 46 ust. 4 i 5 Ustawy o usługach płatniczych. Powyższe przepisy dotyczą zgłaszania przez użytkownika utraty

instrumentu płatniczego, uniemożliwienia korzystania z instrumentu płatniczego po zgłoszeniu jego utraty oraz odpowiedzialności za nieautoryzowane transakcje płatnicze.

Podsumowując, system AMFI może być skonfigurowany w sposób umożliwiający skorzystanie z możliwości wyłączenia w umowie ramowej z użytkownikiem przepisów Ustawy o usługach płatniczych określonych w art. 19 oraz 39 tej ustawy.

8.4. Wyłączenie stosowania Ustawy o usługach płatniczych

Ustawa o usługach płatniczych przewiduje szesnaście przypadków, które powodują wyłączenie jej stosowania. W kontekście elektronicznych płatności przytoczyć należy Art. 6 pkt 11 Ustawy o usługach płatniczych, który określa warunki wyłączenia ustawy w przypadku usług opartych na instrumentach płatniczych, które można wykorzystywać jedynie w ograniczony sposób. Usługi te w celu wyłączenia spod przepisów ustawy powinny spełnić co najmniej jeden z poniższych warunków:

- pozwalają posiadaczowi nabywać towary lub usługi wyłącznie w placówkach wydawców tych instrumentów lub w ramach ograniczonej sieci podmiotów związanych umową handlową bezpośrednio z zawodowym wydawcą tych instrumentów,
- służą wyłącznie do nabywania bardzo ograniczonego zakresu towarów lub usług,
- mogą być używane wyłącznie w jednym państwie członkowskim, jeżeli instrumenty takie są dostarczane na wniosek przedsiębiorcy lub jednostki sektora finansów publicznych, są regulowane ze względu na określone cele społeczne lub podatkowe przez krajowy lub samorządowy organ administracji publicznej i służą do nabycia określonych towarów lub usług od dostawców związanych z wydawcą umową handlową.

W przypadku wdrożenia AMFI jako systemu elektronicznych płatności za usługi oferowane przez polskie jednostki sektora finansów publicznych, istnieją podstawy prawne do wyłączenia stosowania przepisów Ustawy o usługach płatniczych. Na podstawie Art. 6c Ustawy o usługach płatniczych podmiot świadczący usługi płatnicze, który chce skorzystać z wyłączenia stosowania tej ustawy, jest zobowiązany do poinformowania Komisji Nadzoru Finansowego o świadczonych usługach oraz podstawie wyłączenia stosowania Ustawy o usługach płatniczych.

8.5. Wymagania odnośnie do zmiany obowiązujących przepisów

Analiza systemu AMFI w świetle obowiązujących regulacji prawnych pokazuje, że Prawodawca Europejski nie dostosował obowiązujących przepisów do systemów płatności opartych na pieniądzu elektronicznym, który – tak jak w przypadku AMFI – ma postać jednorazowego, elektronicznego znaku pieniężnego. Ponadto, Prawodawca Europejski nie dostosował przepisów do usług płatniczych, które pozwalają na automatyczne dokonywanie anonimowych mikropłatności. **Ze względu na powyższe wnioski, zachodzi konieczność wprowadzenia uregulowań dla anonimowych, zautomatyzowanych mikropłatności przy wykorzystaniu pieniądza elektronicznego**, które powinny uwzględnić:

- wyłączenie stosowania silnego uwierzytelniania podczas inicjowania płatności oraz dokonywania płatności pieniądzem elektronicznym przechowywanym w urządzeniu płatnika (instrumencie płatniczym), jeśli kwota transakcji nie przekracza ustalonego limitu (np. 30 EUR),
- wyłączenie konieczności tworzenia indywidualnych danych uwierzytelniających w bezpiecznym środowisku w przypadku, gdy użytkownik generuje je na swoim urządzeniu, a urządzenie posiada limit maksymalnej kwoty przechowywanych środków (np. 150 EUR), lub doprecyzowanie znaczenia wyrażenia „bezpieczne środowisko” i dookreślenie go jako oprogramowanie działające na urządzeniu użytkownika, uwzględniające aktualne standardy w zakresie bezpieczeństwa systemów informatycznych.

Rozszerzona ekspertyza prawna może ukazać dodatkowe obszary, wymagające zmian w obowiązujących regulacjach prawnych.

8.6. Podsumowanie

Na podstawie analizy przepisów obowiązującego prawa w odniesieniu do systemu anonimowych pikopłatności strumieniowych AMFI, jego wdrożenie jest obecnie możliwe w ograniczonym stopniu jako system płatności za usługi oferowane przez jednostki sektora finansów publicznych, w tym miasta. Powyższe ograniczenie pozwoli na wyłączenie zapisów Ustawy o usługach płatniczych na podstawie art. 6 tej ustawy. Natomiast, aby upowszechnić zastosowanie systemu AMFI jako usługi płatniczej, jest konieczne wprowadzenie zmian regulujących automatyczne mikropłatności z użyciem pieniądza elektronicznego.

W tym rozdziale przedyskutowano szereg wątpliwości i możliwych interpretacji prawnych co do zastosowania pikopłatności w praktyce gospodarczej, w szczególności aspekty związane z anonimowością płatnika (która nie jest elementem koniecznym proponowanego rozwiązania – w docelowej implementacji można z niej zrezygnować). Zapewnienie anonimowości płatnika uniemożliwia zastosowanie silnego uwierzytelniania, wymaganego od usług płatniczych. Dlatego proponowany system należy wdrożyć na podstawie Art. 6 pkt 11 Ustawy o usługach płatniczych, na zasadach wyłączających stosowanie tej ustawy.

Analiza kosztów wdrożenia systemu AMFI



Koszty związane z wdrożeniem systemu AMFI dzielimy na trzy główne grupy:

- koszty związane z przygotowaniem technologii (jednorazowe),
- koszty związane z utrzymaniem infrastruktury po stronie banku,
- koszty związane z przygotowaniem i utrzymaniem infrastruktury po stronie płatnika i odbiorcy płatności.

W ramach pierwszej grupy należy wyraźnie powiedzieć, że w chwili obecnej nie sposób wycenić całościowych kosztów związanych z opracowaniem i przygotowaniem do wdrożenia systemu AMFI. Można jedynie określić wstępnie koszt przygotowania demonstratora technologii, który pokazywałby rozwiązanie problemów technicznych (pokazową implementację systemu w postaci konkretnego sprzętu i oprogramowania). Natomiast nie sposób pokazać kosztów wynikających z dopasowania działania systemu do istniejących i nowych ram prawnych (bez osobnej i szczegółowej ekspertyzy prawnej), kosztów wdrożenia w skali miasta, regionu lub kraju (bez odwołania się do konkretnej firmy, która by się tego podjęła) oraz kosztów codziennej administracji i konserwacji systemu (nie znając skali jego wdrożenia). Z tego względu w tym rozdziale opisano tylko te elementy struktury kosztów, które choć w przybliżeniu (a nawet podając tylko rząd wielkości) można policzyć.

9.1. Koszty związane z przygotowaniem demonstratora technologii

W ramach grupy kosztów związanych z opracowaniem technologii od strony sprzętowej i programowej oraz pokazaniem jej działania w środowisku testowym należy wymienić:

- koszty związane z opracowaniem implementacji testowej protokołów płatności AMFI,
- koszty związane z opracowaniem projektu sprzętowo-programowego oraz stosownych bibliotek do budowy API (ang. Application Programming Interface) do celów łączności mikrosterowników, operujących po stronie odbiorcy płatności, z serwerami po stronie banku,
- koszt opracowania przykładowego mikrosterownika oraz towarzyszącego mu symulatora/demonstratora świadczenia usługi,
- koszty związane z opracowaniem aplikacji na smartfony (w pierwszej kolejności na urządzenia pracujące

pod kontrolą systemu operacyjnego Android w wersji 8 lub nowszej – począwszy od tej wersji zmieniono sposób skanowania transmisji Bluetooth w tle i automatycznego uaktywniania aplikacji po wykryciu takiej transmisji, co znacznie zmniejszyło zapotrzebowanie na energię i uprościło pisanie kodu, a także usprawniło nasłuch sygnałów BLE emitowanych w kanale marketingowym).

Powyższe koszty są kosztami w zasadzie jednorazowymi, choć wiążą się na późniejszych etapach wdrażania systemu z kosztami dostosowania wytworzonego oprogramowania do:

- 1) aktualnej sytuacji prawno-gospodarczej,
- 2) szczegółowych wymagań odbiorców płatności.

Powyższe koszty nie uwzględniają też kosztów specyficznych, ponoszonych przez odbiorców płatności i wynikających z dopasowania ich infrastruktury do specyfiki automatycznych płatności AMFI – takie koszty są praktycznie całkowicie zależne od konkretnego zastosowania systemu i nie sposób ich generalizować. Można jedynie oszacować koszt przygotowania przykładowego stanowiska pokazowego, w podziale na koszt projektu mikrosterownika (indywidualny dla każdego miejsca) i bibliotek API (koszty wspólne dla wszystkich miejsc).

W kolejności, koszty związane z opracowaniem testowej implementacji wymienionych w Rozdziale 7 protokołów AMFI można oszacować na ok. 90 000-110 000 zł. Na koszty te składa się wynagrodzenie wysokiej klasy projektanta i programisty języka Java (ang. senior programmer) w ciągu ok. 6 miesięcy jego pracy, wraz z niezbędnymi opłatami administracyjnymi i podatkowymi oraz utrzymanie środowiska testowego przy wykorzystaniu usług w chmurze obliczeniowej. Końcowym produktem jest zestaw usług REST implementujących protokoły wraz z niezbędną dokumentacją projektową i użytkową.

Koszt opracowania biblioteki w języku C/C++ na potrzeby interfejsu API między mikrosterownikiem i usługami implementującymi protokoły AMFI należy wycenić pod względem nakładów pracy i wymagań podobnie do poprzedniej pozycji – ok. 90 000-110 000 zł, na co składa się głównie wynagrodzenie wysokiej klasy projektanta i specjalisty języka C/C++, znającego środowisko pracy wybranych mikrosterowników. Co do wyboru konkretnej rodziny mikrosterowników, na chwilę obecną można polecić dwa rozwiązania – rodzinę ESP32 firmy Espressif (łączność Bluetooth 4.x oraz WiFi, BLE Mesh, środowisko IDF oraz Eclipse) i rodzinę nRF528xx (Bluetooth 5.x, BLE Mesh, środowisko Segger). W związku z masowym



wdrażaniem technologii 5G należy spodziewać się na rynku – w perspektywie kilku miesięcy – także mikrosterowników lub modułów zdolnych do komunikacji w sieci telefonii komórkowej nowej generacji. W chwili obecnej nie można jeszcze wskazać konkretnych producentów i modeli, nie sposób także ocenić wymagań co do umiejętności programisty i jego znajomości konkretnego środowiska uruchomieniowego.

Na koszt opracowania przykładowego mikrosterownika, poza opisanymi powyżej kosztami przygotowania API, składa się wybór i zakup konkretnego modelu (koszt w detalu nie przekracza 50 zł) oraz niezbędnych modułów wykonawczych (koszt rzędu 50-100 zł), a także koszt opracowania prototypowej płytki montażowej (koszt rzędu 50-200 zł, w zależności od użytej technologii i trwałości oraz wyglądu rozwiązania) i elementów wykonawczych (koszt rzędu kilkuset zł dla typowych serwo mechanizmów) oraz obudowy (wydruk 3D, koszt wraz z opracowaniem ok. 100-300 zł). W sumie koszt przygotowania projektu sprzętowego mikrosterownika wraz z symulatorem instalacji świadczącej usługę (np. podniesienie szlabanu lub sygnalizacja świetlna) nie powinien przekroczyć 1000 zł. Należy zaznaczyć, że w docelowym rozwiązaniu operator płatności będzie ponosić wyłącznie koszty zakupu mikrosterownika (czyli de facto kilkanaście złotych), gdyż cała reszta jego infrastruktury będzie już gotowa do świadczenia danej usługi, pozostanie dołączenie nowego kanału płatności.

Jeśli mikrosterownik miałby wykorzystywać do celów łączności inny kanał komunikacyjny niż BLE, należy także doliczyć koszt dokupienia specjalizowanych modułów łączności. Dla przykładu, koszt zakupu emulatora NFC (jako modułu rozszerzającego możliwości w/w mikrosterownika, np. moduł PN232) to ok. 20-30 zł. Należy zaznaczyć, że wskazane wcześniej mikrosterowniki ESP i nRF bez potrzeby rozbudowy bazy sprzętowej potrafią emulować boje lokalizacyjne w transmisji BLE w kanale marketingowym (jest to kwestia wyłącznie ich oprogramowania), zatem nie wymagają dodatkowych kosztów w tym zakresie (poza kosztami przygotowania stosownego oprogramowania, co jest elementem składowym przygotowania biblioteki API opisanej wcześniej).

Koszty związane z opracowaniem testowej implementacji aplikacji na telefony Android można oszacować na ok. 90 000-110 000 zł. Na koszty te składa się wynagrodzenie wysokiej klasy projektanta i programisty języka Java (ang. senior programmer) w ciągu ok. 6 miesięcy jego pracy, wraz z niezbędnymi opłatami administracyjnymi i podatkowymi. Końcowym produktem jest aplikacja, częściowo działająca w tle i prowadząca nasłuch sygnałów BLE, stanowiąca podstawowy interfejs kontaktu z systemem płatności

oraz pamiętająca wybory i dane personalizacyjne użytkownika, a także przechowująca zakupione w banku pikomony. Ze względu na dużą zmienność rynku smartfonów, celowe jest rozważenie kupna szeregu najnowszych telefonów wiodących producentów (koszt jednostkowy 500-2500 zł za sztukę), w celach jak najszerzego przetestowania systemu.

Podsumowując, przygotowanie demonstratora technologii wymaga zatrudnienia na okres ok. 6 miesięcy trzech wysokiej klasy informatyków (łącznie koszt do 330 000 zł) oraz stosunkowo niewielkich inwestycji sprzętowych (do 20 000 zł). Koszty te nie uwzględniają narzutów wynikających z realizacji umowy, analiz prawnych itp. Pierwsza wersja demonstratora byłaby gotowa w perspektywie ok. 6-9 miesięcy od rozpoczęcia prac, natomiast pełna i przetestowana wersja demonstratora w perspektywie ok. 12 miesięcy. Uwaga – w/w prace programistyczne w dużej mierze mogą być zrównoleglone, ale potem wymagają testów integracyjnych, co wiąże się z wydłużeniem okresu opracowania pełnej wersji demonstratora do wskazanego powyżej roku.

9.2. Koszty związane z utrzymaniem systemu AMFI po stronie banku

Jak wspomniano wcześniej, koszty te są na chwilę obecną praktycznie niemożliwe do oszacowania, choć można pokusić się o wymienienie zakresu czynności, jakie muszą być wykonywane w celu zapewnienia ciągłej pracy systemu. Duża część tych czynności jest związana nie tyle z samym obiegiem pieniądza, co z zapewnieniem zaufania do usług oraz operatorów płatności, w celu umożliwienia ich automatycznej oceny i weryfikacji użyteczności z punktu widzenia konkretnego płatnika.

Grupy czynności i związanych z nimi kosztów związanych z utrzymaniem infrastruktury po stronie banku są następujące:

- koszt udzielenia licencji na system AMFI (do ustalenia na drodze negocjacji z projektantami systemu),
- koszty obliczeń (serwerów, obsługi informatycznej, przelewów itp. – do ustalenia na zasadzie porównania z obecnymi systemami płatności, np. BLIK); obliczenia mogą być wykonywane na istniejących serwerach banku, co zdecydowanie obniży koszty,
- koszty obsługi płatników (odpowiednia strona WWW w serwisie banku, gorąca linia, przeszkolenie pracowników itp.),
- koszty marketingu systemu AMFI,

- koszty bieżącej obsługi aplikacji płatników (rejestracja, automatyczne uaktualnianie kodu oraz danych itp. – do ustalenia w ramach konsultacji z firmą, która będzie zapewniać ciągłość świadczenia usługi AMFI),
- koszty obsługi odbiorców płatności, w tym koszty asysty technicznej i pomocy we wdrażaniu systemu, a także koszty bieżących napraw i usprawnień – do ustalenia w ramach konsultacji z firmą, która będzie zapewniać ciągłość świadczenia usługi AMFI,
- koszty obsługi systemu automatycznej oceny zaufania do usług i związanej z tym certyfikacji elektronicznej (e-podpisów) usług i operatorów płatności – do ustalenia w ramach konsultacji z firmą, która będzie zapewniać ciągłość świadczenia usługi AMFI.

9.3. Koszty po stronie odbiorców płatności (usługodawców)

W zależności od typu odbiorcy płatności oraz jego potrzeb i możliwości wystąpią następujące rodzaje kosztów na etapie wdrożenia systemu AMFI u odbiorców płatności.

1. W przypadku konieczności opracowania i instalacji wyspecjalizowanych urządzeń (odbiorników) do opłat strumieniowych:
 - koszt zakupu odpowiedniej liczby mikrosterowników realizujących funkcje boi lokalizacyjnych zmiennokodowych: ok. 20-30 zł (np. sterownik Nordic Semiconductor lub Espressif ESP-32),
 - koszt zakupu emulatorów NFC, które mogą albo zastąpić boje lokalizacyjne, albo uzupełnić je, zapewniając dodatkowy kanał płatności – ok. 20-30 zł za emulator NFC (np. moduł PN232),
 - koszt opracowania kodu mikrosterownika i implementacji wybranych protokołów jako biblioteki w języku C/C++ – ok. 3 miesiące pracy wysokiej klasy specjalisty (30000-40000 zł, koszt jednorazowy),
 - koszt opracowania aplikacji dla systemu Android – ok. 6 miesięcy pracy wysokiej klasy specjalisty (90000-110000 zł).
2. W przypadku konieczności adaptacji urządzeń świadczących usługi do poboru opłat

strumieniowych (np. podnieść/opuścić szlaban lub włączyć/wyłączyć ładowarkę indukcyjną):

- koszt implementacji kanału zwrotnego przesyłającego potwierdzenia zapłaty z banku i tym samym umożliwiającego automatyczne podejmowanie decyzji o kontynuacji świadczenia usługi – koszt ten będzie silnie zależny od usługi i elementów wykonawczych; jednocześnie jest dość prawdopodobne, że duża część oprogramowania sterującego elementami wykonawczymi będzie już gotowa (bo była wcześniej opracowana na rzecz innych kanałów płatności) i na przykład pozostanie tylko usługa pobierania informacji o wniesieniu opłaty z banku,
 - koszt implementacji niezbędnych procedur weryfikacyjnych, które umożliwiają odróżnienie klientów wnoszących opłaty automatyczne od „tradycyjnych”, korzystających z aktualnych sposobów dokonywania płatności. Dla przykładu, będzie to koszt kontrolerów, którzy sprawdzają wnoszenia opłat dla zaparkowanych samochodów na podstawie ich numerów rejestracyjnych. Koszt ten jest już prawdopodobnie poniesiony przez operatora usługi, gdyż czynności weryfikacyjne są niezbędne do świadczenia usługi także w formie tradycyjnej. Koszt ten można też zmniejszyć, rezygnując z pracy ludzkiej na rzecz wykorzystania automatów lub półautomatów (np. kontroler ręcznie sprawdza tylko te samochody, które nie raportują przez łącze BLE wniesienia opłaty).
3. W przypadku przyjmowania płatności strumieniowych za pomocą transmisji w sieci lokalnej lub rozległej:
 - poza omówionymi w punkcie drugim powyżej kosztami adaptacji urządzeń wykonawczych, w grę mogą wchodzić koszty transmisji sieciowej do/z mikrosterowników i urządzeń wykonawczych, oraz niezbędne serwery (w sieci lokalnej i chmurze) i usługi. Większość z nich jest prawdopodobnie niezbędna dokładnie w takiej samej formie przy wykorzystaniu płatności tradycyjnej (która wymaga zaufanej transmisji w sieci lokalnej i rozległej), dlatego raczej nie należy się tu spodziewać dużych wydatków związanych z dostosowaniem tego oprogramowania do pracy z systemem AMFI.

Na etapie eksploatacji systemu AMFI przez odbiorców płatności należy także uwzględnić koszt świadczenia usługi przez bank odbiorcy płatności.



Możliwości wdrożenia systemu AMFI w inteligentnych miastach



Jak wcześniej wspomniano, system AMFI ma charakter uniwersalny i może być użyty wszędzie tam, gdzie są zamontowane odbiorniki płatności strumieniowych. AMFI zapewnia ten sam poziom uniwersalności, co karty płatnicze lub BLIK, które również mogą być użyte do zapłaty za wszystkie produkty lub usługi pod warunkiem, że towarzyszy im odpowiedni odbiornik płatności. Konieczne jest jednak podkreślenie, że zakres systemu AMFI jest ograniczony do realizacji płatności, nie obejmuje natomiast funkcji związanych z samą usługą – dokładnie tak samo, jak takich funkcji nie obejmują odbiorniki płatności kartami lub Blikiem. Jeśli z płatną usługą jest związane podniesienie szlabanu, to konieczne jest oprzyrządowanie i oprogramowanie tej funkcji, a następnie powiązanie jej z AMFI. Podobnie, jeśli z usługą jest związane zdalne uruchomienie lub unieruchomienie silnika, np. elektrycznej hulajnogi, to taka funkcja musi być oprzyrządowana i oprogramowana, a następnie powiązana z AMFI. Należy zakładać, że – tak jak to ma miejsce obecnie – za różne usługi będzie można płacić w różny sposób, nie tylko za pomocą AMFI. Zachętą do płatności za pomocą AMFI przez płatników (usługobiorców) jest strumieniowość zapewniająca opłatę proporcjonalną do czasu świadczenia usługi. Dla usługodawców zaletą AMFI jest zwiększone zainteresowanie usługami, bo usługobiorcy będą chętniej korzystać z usług wiedząc, że jeśli z jakiegokolwiek powodu zrezygnują z danej usługi w trakcie jej świadczenia, to poniosą koszty tylko za faktyczny czas, w którym z niej korzystali.

Jak wspomniano w Rozdziale 3, płatności za pomocą systemu AMFI można generalnie podzielić na:

- płatności za używanie pewnego urządzenia przez określony czas,
- płatności za przebywanie w danym miejscu, przy czym jedną z motywacji do wprowadzenia płatności w tym przypadku może być chęć ograniczenia liczby ludzi przebywających w tym miejscu.

System AMFI daje możliwość zróżnicowania płatności za usługi publiczne dla mieszkańców (płatników lokalnych podatków) i przyjezdnych (mieszkańców okolicznych gmin, turystów):

- mieszkańcy mogą płacić strumieniowo, ale po preferencyjnej cenie,
- mieszkańcy, którzy nie płacą strumieniowo, płacą w tradycyjnych punktach poboru opłat, tracąc korzyści z opłat proporcjonalnych do czasu świadczenia usługi,
- przyjezdni płacą – wygodnie strumieniowo, niewygodnie w tradycyjnych punktach poboru.

Najłatwiejsze jest zastosowanie AMFI w usługach czysto cyfrowych, takich jak na przykład wideo na żądanie. Usługobiorca zaczyna oglądać film, za który płaci za pomocą AMFI. Jeśli film mu się nie spodoba lub z jakiegokolwiek powodu musi przerwać oglądanie, to zapłaci tylko za obejrzaną część. Tego typu model biznesowy będzie zachęcał do oglądania filmów w formacie wideo na żądanie, bo redukuje ryzyko zapłaty za nieobejrany film. Podobny obszar zastosowań to gry komputerowe, w których można dodatkowo dynamicznie zmieniać wysokość opłat w zależności od uzyskiwanych wyników, co stanowiłoby dodatkową motywację do grania.

Zastosowanie systemu AMFI do korzystania z urządzeń fizycznych musi być związane z obsługą tego urządzenia z uwzględnieniem jego specyfiki. Na przykład, elektryczna hulajnoga może odblokować się natychmiast po skierowaniu do niej strumienia pikopłatności. Jeśli użytkownik hulajnogi stanie i odejdzie od niej, to strumień pikopłatności automatycznie zakończy się. Jeśli jednak w trakcie jazdy użytkownik przestanie płacić strumieniem pikopłatności – bo skończył mu się rulon pikomonet lub wyłączył swój telefon – to hulajnoga powinna się zablokować. Nie może tego jednak zrobić gwałtownie i bez ostrzeżenia, bo mogłoby dojść do wypadku. Wypożyczalnie hulajnóg już w tej chwili stosują taki system auto-wyłączania w sytuacji utraty łączności z urządzeniem.

Przy uwzględnieniu specyfiki każdego urządzenia można stosować system AMFI do rowerów miejskich (pod warunkiem wbudowania w nich zdalnego blokowania), współdzielonych samochodów miejskich (wyposażonych w zdalny immobilizer), urządzeń do ćwiczeń gimnastycznych w publicznych parkach itp. W przyszłości system AMFI będzie mógł być stosowany do opłat za indukcyjne ładowanie samochodów elektrycznych na miejscach parkingowych.

System AMFI można też stosować w wypożyczalniach sprzętu wypoczynkowo-rekreacyjnego, na przykład leżaków, parawanów i koszy na plaży, łódek, kajaków, atrakcji w lunaparku, wejścia do strefy specjalnej typu spa lub sauna itp. W takim przypadku nie ma jednak możliwości zablokowania korzystania z wypożyczonej rzeczy lub atrakcji po ustaniu strumienia pikopłatności. Fakt ten jednak można łatwo wykryć i sygnalizować odpowiednim służbom z prośbą o reakcję. Taki sposób wykrywania braku opłaty i reakcji na ten fakt jest już w tej chwili standardem i nie będzie wymagać większych zmian organizacyjnych w świadczeniu usługi wypożyczenia.

Do kategorii zastosowań systemu AMFI do płatności za przebywanie w danym miejscu należy opłata za przejazd tramwajem lub autobusem proporcjonalna



do czasu jazdy. Pasażer po wejściu do tramwaju lub autobusu automatycznie zaczyna płać strumieniowo, a po wyjściu – automatycznie przestaje. Kontrola wniesienia opłaty w systemie AMFI może być realizowana klasycznie (na życzenie kontrolera trzeba okazać ekran aplikacji z potwierdzeniem wniesienia opłaty za cały czas przebywania w pojeździe, tak jak to jest w tej chwili wykonywane np. w aplikacji MoBilet) lub można wykorzystać aplikację do automatycznego rozgłaszania w sieci BT Mesh potwierdzenia wniesienia opłaty. Ten drugi sposób zapewnia anonimowość płatnika i umożliwia automatyczne odróżnianie osób, które opłaciły przejazd od tych, które tego nie zrobiły i których smartfony nie emitują stosownego sygnału. W przypadku tłoku i niemożności odróżnienia transmisji z telefonów poszczególnych pasażerów można wykorzystać kontrolę klasyczną w stosunku do wszystkich osób w danym miejscu.

Strumieniowo można płać za zwiedzanie zabytków i muzeów. Opłata strumieniowa może być pobierana za sam fakt przebywania na terenie zabytku lub muzeum. Można też połączyć opłatę za zwiedzanie z systemem elektronicznych przewodników. Przy danym dziele sztuki lub obiekcie muzealnym może być umieszczona elektroniczna boja AMFI. Jeśli zwiedzający skieruje strumień pikopłatności do tej boi, to otrzyma możliwość odtworzenia na swoim smartfonie audycji multimedialnej na temat oglądanego obiektu.

System AMFI można też stosować na otwartym terenie, różnicując przy tym opłaty dla mieszkańców i przyjezdnych:

- wejście do parku,
- wejście na plac zabaw,
- wejście na deptak,
- wejście na plażę miejską.

W takim przypadku kontrola wnoszenia opłat powinna być realizowana w sposób klasyczny, z możliwością automatycznej identyfikacji osób, które wniosły opłatę w sieci BT Mesh, tak jak to opisano w przypadku weryfikacji opłat za przejazdy komunikacją miejską.

System AMFI może też służyć do wnoszenia opłat za miejsca parkingowe w mieście. Jeśli z każdym miejscem zostanie związana boja, to jej sygnał może zainicjować płatność w momencie, gdy pojazd zatrzyma się w tym miejscu i zakończyć wnoszenie opłat, gdy pojazd odjedzie. Opłaty mogą być wnoszone albo przez komputer pokładowy samochodu (transmisja BLE), albo za pośrednictwem smartfonu (transmisja

w sieci rozległej, smartfon nie musi znajdować się w pobliżu zaparkowanego samochodu). Ten drugi sposób wymaga pewnej interakcji z użytkownikiem (choćby w celu deklaracji kierowcy – powiązania smartfonu z numerem rejestracyjnym pojazdu) albo połączenia smartfonu i komputera pokładowego wspólną aplikacją (np. Android Auto).

Ciekawym zastosowaniem systemu AMFI w inteligentnym mieście mógłby być płatny wjazd do ścisłego centrum miasta, który ma na celu rozładowanie korków oraz ograniczenie emisji spalin i hałasu. Rozwiązanie takie, ale oparte na innej technologii, jest stosowane w Londynie. Londyński system działa w taki sposób, że – generalnie – za wjazd do centrum trzeba uiścić stałą opłatę dzienną [Londynek.net 2018]. Po zapłaceniu można przebywać w centrum dowolnie długo oraz wjeżdżać i wyjeżdżać w ciągu dnia dowolnie wiele razy. Płatności dokonuje się przelewem lub opłata jest pobierana automatycznie po zarejestrowaniu się w odpowiednim systemie informatycznym. Technicznie system działa na zasadzie identyfikacji tablic rejestracyjnych pojazdów. Jeśli system zidentyfikuje pojazd w centrum, a kierowca nie uiści opłaty, to otrzymuje mandat karny. Pojazdy wyróżnionych kategorii są zwolnione z opłat, a pojazdy ekologiczne mają opłatę obniżoną.

Wprowadzenie systemu pikopłatności strumieniowych AMFI spowodowałoby, że kierowcy wjeżdżający do centrum miast i wnoszący opłaty w zależności od czasu przebywania w tym miejscu byłiby zainteresowani jak najkrótszym przebywaniem w nim w celu ograniczenia kosztów. Dzięki temu kierowcy optymalizowaliby koszty, a miasto realizowało swoje cele dotyczące ograniczenia korków, emisji spalin i hałasu, nadal mając ważne źródło przychodu. System AMFI pozwoliłby na zróżnicowanie opłat dla mieszkańców miasta (płatników lokalnych podatków) i przyjezdnych. Z jednej strony zachęcałoby to osoby często przyjeżdżające do miasta – np. ze względu na pracę – do deklarowania podatków lokalnych w tym mieście, a z drugiej zmniejszyłoby opór mieszkańców przed wprowadzeniem opłat za wjazd do centrum, w tym przejazd przez centrum. System AMFI pozwoliłby także na dynamiczne zróżnicowanie opłat – w przypadku przekroczenia pewnej liczby pojazdów w centrum miasta opłaty byłyby automatycznie podnoszone, a aplikacja AMFI powiadamiałaby o tym fakcie kierowców.

Problem pobierania opłat za wjazd samochodem do ścisłego centrum miasta nie może być rozwiązany za pomocą samego systemu AMFI, ze względu na potencjalną trudność wykrywania samochodów, które przebywają w centrum, ale nie płacą. Dlatego system AMFI mógłby być uzupełnieniem systemu

rozpoznawania tablic rejestracyjnych i klasycznego sposobu wnoszenia opłat. Zachętą dla kierowców byłyby opłaty zależne od czasu przebywania w centrum miasta, potencjalnie znacznie niższe niż dzienny abonament. Jednocześnie zwiększenie liczby samochodów, których kierowcy zdecydują się na taki system opłat, nie tylko nie zmniejszyłoby, ale raczej zwiększyłoby przychody miasta.

Warto zauważyć, że wdrożenie systemu AMFI w różnych miastach, które chciałyby ograniczyć wjazd od swoich centrów, nie wiązałoby się dla kierowców z żadnymi dodatkowymi trudnościami. W każdym mieście, ta sama aplikacja mobilna AMFI umożliwiałaby im dokonywanie płatności strumieniowych.

Po wprowadzeniu systemu AMFI w centrach miast i zapoznaniu się z aplikacją przez wielu mieszkańców i przyjezdnych celowe byłoby jej używanie w innych zastosowaniach w inteligentnym mieście.

Należy jednak zaznaczyć, że wprowadzenie systemu opłat za wjazd do ścisłego centrum miasta wymaga osobnego studium wykonalności, gdyż jest to usługa bardzo skomplikowana z punktu widzenia organizacji i weryfikacji wnoszenia opłat.

System AMFI mógłby też znaleźć zastosowanie w sektorze prywatnym, jednak pod warunkiem rozwiązania kwestii prawnych, o których mowa w Rozdziale 8. Warto byłoby wprowadzić płatności strumieniowe na przykład w klubach i dyskotekach, dzięki czemu klient mógłby sprawdzić np. przez pół godziny, czy chce zostać dłużej, ponosząc koszt tylko faktycznej obecności na imprezie. Innym obszarem zastosowań są bary szybkiej obsługi, którym zależy na szybkiej rotacji klientów. Opłata mogłaby być hybrydowa – tradycyjna opłata za dania i strumieniowa opłata za czas spędzony w barze.

System AMFI cechuje duża odporność na cyberataki. W najgorszym przypadku przejęcie przez cyberatakującego kontroli nad płatnościami spowoduje brak opłat, ale same usługi pozostaną w pełni funkcjonalne. Pikomonyety można do pewnego momentu weryfikować off-line, dopiero ich zamiana na pieniądze rzeczywiste wymaga łączności z bankiem. Zatem nie zachodzi możliwość paraliżu miasta, a jedynie możliwość pewnych strat finansowych dla miasta lub banku, w zależności od przyjętej polityki rozliczeń. Takie uniemożliwienie świadczenia usługi lub przejęcie opłat można stosunkowo szybko wykryć

i neutralizować, co pokazuje dzisiejsza praktyka np. w zakresie wnoszenia opłat za przejazdy komunikacją miejską, parkingi miejskie itp. Podobnie ataki typu „masowy dostęp”, które blokują serwery bankowe samą liczbą zgłoszeń, są mało skuteczne w proponowanym systemie – atakujący musiałby przejąć kontrolę nad każdym punktem świadczenia usługi osobno, co przy dużej liczbie punktów jest praktycznie niemożliwe. Można to porównać do sytuacji, w której ktoś atakuje wszystkie bankomaty w mieście, aby uniemożliwić wypłatę gotówki w całym mieście. Taki atak bardzo trudno zsynchronizować – wszystkie punkty musiałyby być zaatakowane praktycznie równocześnie, inaczej pierwsze ataki spowodują alarm i uruchomią procedury neutralizacyjne. Zatem to ryzyko jest niskie i jest związane raczej z możliwością blokady konkretnego punktu świadczenia usług, a nie całego systemu.

Może się także wydawać, że niebezpieczeństwem jest oferowanie przez osoby i firmy niezwiązane z miastem fikcyjnych usług, za które byłyby pobierane rzeczywiste opłaty. Skoro takie usługi byłyby obsługiwane automatycznie, czyli bez bezpośredniego nadzoru płatników, to na pierwszy rzut oka można pomyśleć, że może to powodować duże straty, nie tylko finansowe, także w wizerunku i zaufaniu do miasta lub banku. Jednak taka możliwość jest bardzo mało prawdopodobna z kilku względów. Po pierwsze, w raporcie sugeruje się, aby każda nowa usługa podlegała weryfikacji przez płatnika – dostaje on ostrzeżenie, że nigdy wcześniej z takiej usługi nie korzystał i musi się na nią zgodzić. Dopiero po uzyskaniu zgody następne opłaty za taką usługę są realizowane w pełni automatycznie. Po drugie, w raporcie proponuje się limit płatności (dzienny, tygodniowy, miesięczny, związany z typem usługi itp.), zatem takie ryzyko odpowiadałoby poziomowi ryzyka dzisiejszych kart bezstykowych i płatności za pomocą smartfonów, do czego klienci banku są już przyzwyczajeni i co akceptują. Po trzecie, w raporcie sugeruje się, aby wszystkie usługi były autoryzowane przez bank (albo inną jednostkę wysokiego zaufania społecznego, na przykład miasto) za pomocą podpisu cyfrowego. Autorom raportu nie jest znany przypadek naruszenia procedur weryfikacji podpisów, poza ich wyłudzeniem (co jednak można eliminować na drodze administracyjnej, a także wprowadzając „czarną listę” podpisów oszustów, znaną aplikacji płatnika i często uaktualnianą na tej samej zasadzie, jak bazy danych wirusów w pakiecie antywirusowym). Zatem ryzyko związane z wyłudzeniem opłat za „fałszywe” usługi należy uznać za bardzo niskie.



Propozycja dalszych badań



System pikopłatności strumieniowych AMFI szczegółowo opisany w tym raporcie znajduje się obecnie na III poziomie gotowości technologicznej (ang. Technology Readiness Levels – TRL) [Rozporządzenie MNiSW 2011/18/91]. Poziom III TRL oznacza, że „potwierdzono analitycznie i eksperymentalnie krytyczne funkcje i/lub koncepcje technologii. Oznacza to przeprowadzenie badań analitycznych i laboratoryjnych mających na celu potwierdzenie przewidywań badań naukowych wybranych elementów technologii. Między innymi należy do nich zaliczyć przykłady obejmujące komponenty, które nie są jeszcze zintegrowane w całość lub też nie są reprezentatywne dla całej technologii.”

W celu dalszego rozwoju systemu AMFI jest konieczne wykonanie prototypu, który osiągnąłby poziom VI TRL, który oznacza: „demonstrację prototypu lub modelu systemu albo podsystemu technologii w warunkach zbliżonych do rzeczywistych. Oznacza to, że przebadano reprezentatywny model lub prototyp systemu, który jest znacznie bardziej zaawansowany od badanego na poziomie V, w warunkach zbliżonych do rzeczywistych. Poziom ten reprezentuje znaczący krok naprzód w zademonstrowanej gotowości technologii. Należy do nich zaliczyć badania prototypu w warunkach laboratoryjnych odwzorowujących z dużą wiernością warunki rzeczywiste lub w symulowanych warunkach operacyjnych.”

System mógłby być dalej rozwijany ze środków jednego banku lub konsorcjum banków. Jest też celowe rozważenie złożenia wniosku o finansowanie projektu do NCBR przez odpowiednie konsorcjum, w skład którego wchodziłby Uniwersytet Ekonomiczny w Poznaniu, jeden lub kilka banków lub instytucji bezpośrednio współpracujących z bankami, doświadczony deweloper oprogramowania dla potrzeb banków oraz przedstawiciele usługodawców, którzy pobieraliby opłaty za pomocą systemu AMFI. Projekt taki miałby

szanse na dofinansowanie, gdyż wpisuje się w Krajowe Inteligentne Specjalizacje [Ministerstwo Rozwoju 2020].

KIS 10. Inteligentne sieci i technologie informacyjno-komunikacyjne oraz geoinformacyjne.

Rozdział I. Technologie internetu przyszłości, technologie Internetu Rzeczy, systemy wbudowane

Punkt 5. Rozwiązania Internetu Rzeczy (ang. Internet of Things)

Rozdział II. Inteligentne sieci w infrastrukturach

Punkt 1: Inteligentne miasta (ang. smart cities)

Punkt 4. Inteligentne systemy transportowe (ang. smart/intelligent transportation systems)

Punkt 5. Inteligentne pojazdy (ang. smart vehicles)

Kolejnym etapem prac nad pikopłatnościami strumieniowymi powinno być zaprojektowanie demonstratora technologii, czyli de facto w pełni funkcjonalnego prototypu systemu, pracującego w warunkach symulowanych (na przykład z modelami urządzeń typu automatyczne drzwi lub szlaban, ale już z rzeczywistymi smartfonami i kanałami łączności). Symulowany byłby także udział banku – w demonstratorze uruchomiony powinien być obieg pieniądza symulowanego, o cechach jak najbardziej zbliżonych do rzeczywistych środków płatniczych, dostępny przez obecnie wykorzystywane przez banki protokoły wymiany danych i systemy zabezpieczeń. Należy zaznaczyć, że oprogramowanie demonstratora byłoby przygotowane według założeń projektowych pozwalających w przyszłości na dość łatwe przeniesienie demonstratora do pracy w warunkach rzeczywistych.



Bibliografia

- Bajor B., Byrski J., Zalcewicz A. 2017 – Ustawa o usługach płatniczych. Komentarz, wydanie II, Wolters Kluwer
- CCITSE 2012 – Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, v 3.1 rev. 4, CCMB 2012, on-line: <https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf>
- Deloitte 2015a – Payments disrupted: The emerging challenge for European retail banks, Deloitte, on-line: <https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/financial-services/payments-disrupted-2015.pdf>
- Deloitte 2015b – Smart Cities: How rapid advances in technology are reshaping our economy and society, Deloitte The Netherlands, on-line: <https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/public-sector/deloitte-nl-ps-smart-cities-report.pdf>
- Deloitte 2017 – Smart City Smart Nation: Providing the keys to unlock your city's potential, Deloitte Development, online: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-cons-deloitte-smart-city-trends-and-case-studies.pdf>
- Deloitte 2018 – Delivering the digital city: Building a best-in-class customer experience in smart cities, Deloitte Development, online: <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Public-Sector/gx-ps-dcgi-delivering-the-digital-city.pdf>
- ISO 2015 – Smart cities: Preliminary Report 2014, ISO/IEC, online: https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/smart_cities_report-jtc1.pdf
- Londynek.net 2018 – Congestion Charge: Opłaty za wjazd do centrum Londynu, on-line: https://londynek.net/ukipedia/article?jdnews_id=4156510
- McKinsey 2018 – Smart Cities: Digital solutions for a more livable future, McKinsey&Company, online: <https://www.mckinsey.com/~media/mckinsey/industries/capital%20projects%20and%20infrastructure/our%20insights/smart%20cities%20digital%20solutions%20for%20a%20more%20livable%20future/mgi-smart-cities-full-report.ashx>
- Ministerstwo Rozwoju 2020 – Krajowe Inteligentne Specjalizacje, online: <https://www.gov.pl/web/rozwoj/krajowe-inteligentne-specjalizacje>
- Orlen 2020 – Płać z ORLEN PAY, on-line: <http://www.vitay.pl/O-programie/Plac-z-ORLEN-PAY,84.html>
- PEKA 2020 – tPortmonetka – karta imienna, Poznańska Elektroniczna Karta Aglomeracyjna, online: <https://www.peka.poznan.pl/web/porta1/tportmonetka1>
- PwC 2019 – Creating the smart cities of the future: A three-tier development model for digital transformation of citizen services, PwC, online: <https://www.pwc.com/gx/en/sustainability/assets/creating-the-smart-cities-of-the-future.pdf>
- Rozporządzenie KE 2018/389 – Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji, Dziennik Ustaw UE L.2018.69.23 z dnia 2018.03.13
- Rozporządzenie MNiSW 2011/18/91 – Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 4 stycznia 2011 r. w sprawie sposobu zarządzania przez Narodowe Centrum Badań i Rozwoju realizacją badań naukowych lub prac rozwojowych na rzecz obronności i bezpieczeństwa państwa, Dz.U.2011.18.91 z dnia 2011.01.27
- Sturm M. 2018 – Rachel Botsman: An Economy of Trust, Nordic Business Report, online: <https://www.nbforum.com/nbreport/rachel-botsman-economy-trust/>
- Sujata J., Saksham S., Tanvi G., Shreya D. 2016 – Developing smart cities: an integrated framework w:



Procedia Computer Science, vol. 93, s. 902-909, Elsevier

TFL 2020a – Transport For London: Contactless and mobile pay as you go, on-line: <https://tfl.gov.uk/fares/how-to-pay-and-where-to-buy-tickets-and-oyster/pay-as-you-go/contactless-and-mobile-pay-as-you-go>

TFL 2020b – Transport For London: Touching in and out, on-line: <https://tfl.gov.uk/fares/how-to-pay-and-where-to-buy-tickets-and-oyster/pay-as-you-go/touching-in-and-out>

Ustawa 2019/1781 – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dziennik Ustaw 2019 poz.1781

Ustawa 2020/794 – Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, Dziennik Ustaw 2020 poz. 794

WEF 2018 – Circular Economy in Cities: Evolving the model for a sustainable urban future, World Economic

Forum, online: http://www3.weforum.org/docs/White_paper_Circular_Economy_in_Cities_report_2018.pdf

Woetzel J., Remes J. 2018 – Is Your Company Ready for the Rise of Smart Cities?, Harvard Business Review, online: <https://hbr.org/2018/06/is-your-company-ready-for-the-rise-of-smart-cities>

Yamabe T., Lehdonvirta V., Ito H., Soma H., Kimura H., Nakajima T. 2010 – Activity-based micropricing: realizing sustainable behavior changes through economic incentives, w: International Conference on Persuasive Technology, s. 193-204, Springer

ZTM 2020 – Vademecum biletowe, Zarząd Transportu Miejskiego, on-line: <https://www.ztm.poznan.pl/pl/cennik/cennik/vademecum-biletowe/>

Zuccherato R. 2011 – Entity Authentication, w: van Tilborg H.C.A., Jajodia S. (red.) Encyclopedia of Cryptography and Security, s. 420-421, Springer