UseCrypt.
Bringing
privacy back.

PREZENTACJA INWESTORSKA

Październik, 2019

NINIEJSZY MATERIAŁ MA CHARAKTER

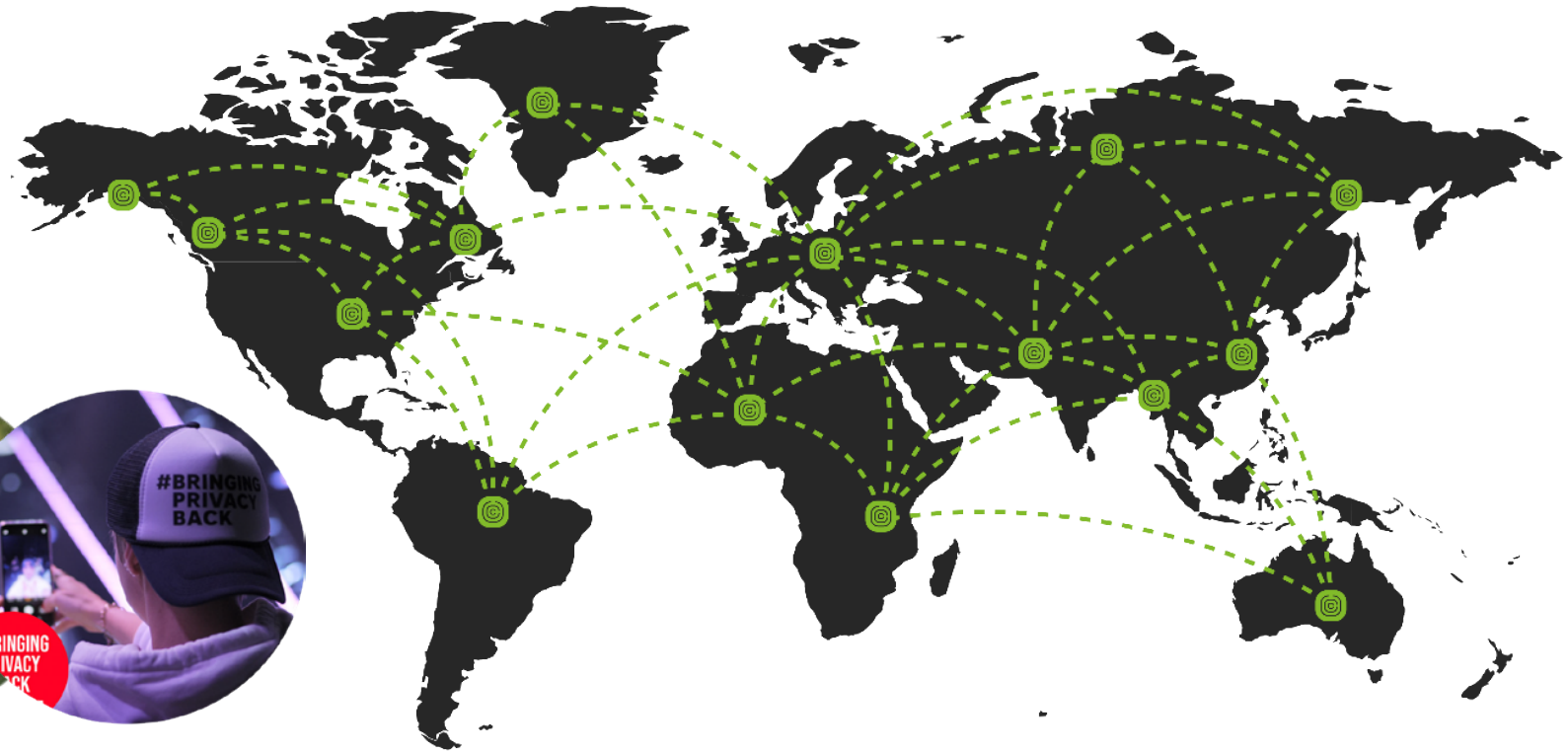
WYŁĄCZNIE PROMOCYJNY.

JEDYNYMI WIĄŻĄCYMI DOKUMENTAMI SĄ
WARUNKI EMISJI OBLIGACJI
ORAZ DOKUMENT INFORMACYJNY,
ZNAJDUJĄCE SIĘ NA STRONIE EMITENTA.

Nasza firma oferuje trzy produkty zmieniające zasady szyfrowania w chmurze, których zadaniem jest zastąpienie tradycyjnych, firmowych e-maili, rewolucja w przechowywaniu plików oraz oferowanie prawdziwie bezpiecznego standardu komunikacji

USECRYPT

#BRINGINGPRIVACYBACK



NASZĄ MISJĄ JEST PRZYWRÓCENIE PRYWATNOŚCI I ODDANIE JEJ W RĘCE UŻYTKOWNIKA. WIZJA USECRYPT POLEGA NA STWORZENIU GLOBALNEJ SPOŁECZNOŚCI, KTÓRĄ SPAJA PRAWDZIWA PRYWATNOŚĆ.

PONAD MILION OSÓB ZOBACZYŁO NASZ MANIFEST

https://www.youtube.com/watch?v=PlTOfyPHbCU

KLUCZOWE WNIOSKI

USECRYPT

O USECRYPT

- Dynamicznie rozwijający się dostawca unikalnych rozwiązań z zakresu szyfrowania i cyberbezpieczeństwa.
- Opatentowana technologia szyfrowania Usecrypt: Hybrid Virtual Key Management – struktura klucza wirtualnego, w ramach której klucze szyfrowania zachowują odrębność, co zapobiega nieupoważnionemu dostępowi do danych.
- Trzy opracowane produkty: w pełni szyfrowana aplikacja desktopowa do udostępniania plików (Usecrypt Safe), w pełni szyfrowana poczta elektroniczna (Usecrypt Mail) oraz mobilny komunikator (Usecrypt Messenger), który jest wdrażany globalnie.
- Dynamiczny zespół ds. zarządzania z doświadczeniem w rozwoju firm i silnymi kompetencjami z zakresu kryptologii.
- Po okresie szybkiego wzrostu na rynku polskim (26 tys. użytkowników i 11 mln PLN przychodów) Usecrypt globalnie skaluje swój model biznesowy.
- Usecrypt miał już kilka rund finansowania kapitału zakładowego (podczas których zgromadził 3,1 mln USD) i czerpie korzyści z silnego wsparcia ze strony funduszu private equity.

KLUCZOWE PRZEWAGI

Rozwiązania technologiczne	Przełomowa, w pełni autorska i opatentowana technologia Hybrid Virtual Key Management („HVKM”) to najbezpieczniejsze rozwiązanie z zakresu udostępniania plików i komunikacji.
Dynamika rynku cyberbezpieczeństwa	Brak skutecznych rozwiązań z zakresu szyfrowania danych oraz zwiększone zagrożenie ze strony cyberataków i wycieków danych stymulują popyt na rozwiązania Usecrypt.
Potencjał rynkowy	Wykorzystanie potencjału rynkowego czterech dynamicznie rozwijających się sektorów: przechowywania danych w chmurze, firmowej poczty elektronicznej, bezpieczeństwa stacji roboczych oraz urządzeń mobilnych.
Skalowalny model biznesowy	Model biznesowy oparty na miesięcznych subskrypcjach (SaaS) oraz wdrożeniach on-premise

KAMIENIE MILOWE FIRMY

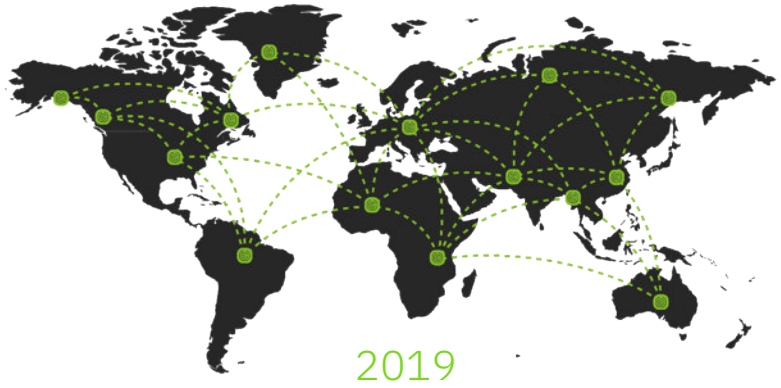
USECRYPT

Usecrypt skutecznie skomercjalizował swoją opatentowaną technologię, uruchomił sprzedaż produktów w Polsce, a obecnie pracuje nad sprzedażą międzynarodową.

1 Wprowadzenie produktu na rynek i prowadzenie sprzedaży w Polsce

2 Wejście na rynki globalne

Wejście na rynki globalne w 12 krajach



KLUCZOWE PRODUKTY

USECRYPT

Dzięki technologii HVKM Usecrypt opracował produkty, które zmieniają zasady szyfrowanej komunikacji (brak pośrednika w procesie).

USECRYT MESSENGER

Mobilny komunikator oferujący w pełni zabezpieczone połączenia HD, wiadomości tekstowe, rozmowy grupowe oraz wymianę plików multimedialnych

Dostępny w Google Play oraz AppStore

USECRYPT SAFE

Usecrypt Safe to aplikacja desktopowa, która szyfruje dane podczas połączenia z serwerem przy użyciu technologii HVKM. Dzięki szyfrowaniu end to end możesz bezpiecznie przechowywać, udostępniać i przesyłać swoje pliki

USECRYPT MAIL

W pełni szyfrowana usługa poczty elektronicznej Usecrypt oparta na technologii HVKM wzbogacona o plug-in dla Microsoft Outlook.

Produkt w fazie wejścia na rynek

ZAUFALI NAM

USECRYPT

Partnerzy strategiczni	DELL, IBM, NETIA
Nagrody i certyfikaty	Deloitte., COMPUTERWORLD, INSTYTUT ŁĄCZNOŚCI PAŃSTWOWY INSTYTUT BADAWCZY, WAT Military University of Technology
Kluczowi klienci	Unipetrol ORLEN GROUP, GROM, EY, GRUPA CAPITAL PARK RAZEM TWORZYMY WARTOŚĆ, SOP, G4S, SOLIDARNOŚĆ, POLSKA PRESS GRUPA, BR Narodowe Centrum Badań i Rozwoju

UNIKALNE POŁĄCZENIE KLUCZOWYCH KOMPETENCJI

USECRYPT

Polska akademicka baza kryptograficzna oraz skuteczny dział operacyjny, połączone z centrum R&D w Izraelu przy wsparciu doświadczonych inwestorów, dają możliwość skalowalnych wdrożeń globalnych.

30
Wielkość zespołu

JAKUB SIERAKOWSKI

Członek Zarządu Usecrypt S.A.
Ekspert z zakresu bezpieczeństwa informacji i systemów ochrony danych

YUVAL RABIN

Członek Rady Nadzorczej Usecrypt S.A
Weteran rynku IT z ponad 40 letnim doświadczeniem

MIKE MAYER

Członek Rady Nadzorczej
Ex-SAP, ex-ORACLE; ponad 30 lat doświadczenia w globalnym świecie korporacyjnego IT

ZESPÓŁ DS. KLUCZOWYCH TECHNOLOGII

USECRYPT

Zespół ds. Usecrypt Safe & Usecrypt Mail

JAKUB ŻURKOWSKI
Dyrektor ds. Technicznych Usecrypt Safe Ex-Samsung

PAWEŁ NAZAREWSKI
Szef Cloud Infrastructure Maintenance Wojskowa Akademia Techniczna w Warszawie

PRZEMYSŁAW CIĘŻKOWSKI
Starszy programista C++, Ex Samsung

KRZYSZTOF BOROWIEC
Starszy programista C++, Politechnika Warszawska

ADRIAN OSAK
Programista C++

MIKOŁAJ DZIEŁ
Technology Tester

KLAUDIA WIJAS
Technology Tester

Zespół ds. Usecrypt Messenger

KAMIL KACZYŃSKI
Dyrektor ds. Technicznych Usecrypt Messenger
Doktor, Wojskowa Akademia Techniczna w Warszawie

MICHAŁ GLET
Szef zespołu programistów Usecrypt Messenger

KLUCZOWE INFORMACJE FINANSOWE

26TYS / **7,0MLN**

Liczba użytkowników

Przychody na koniec 2018, PLN

0.3MLN

EBITDA
Na koniec 2018, PLN

01

POTENCJAŁ RYNKOWY ORAZ CZYNNIKI WZROSTU

POWTARZAJĄCE SIĘ WYCIEKI PRYWATNYCH DANYCH

USECRYPT

Brak skutecznych rozwiązań, które gwarantują pełną prywatność komunikacji oraz ochronę danych przed hakerami

Wielki atak hakerski: jak Chiny przy pomocy niewielkiego chipa dokonały infiltracji amerykańskich firm

Bloomberg Businessweek

FBI odzyskuje dane z aplikacji WhatsApp i Signal z telefonu Michaela Cohena

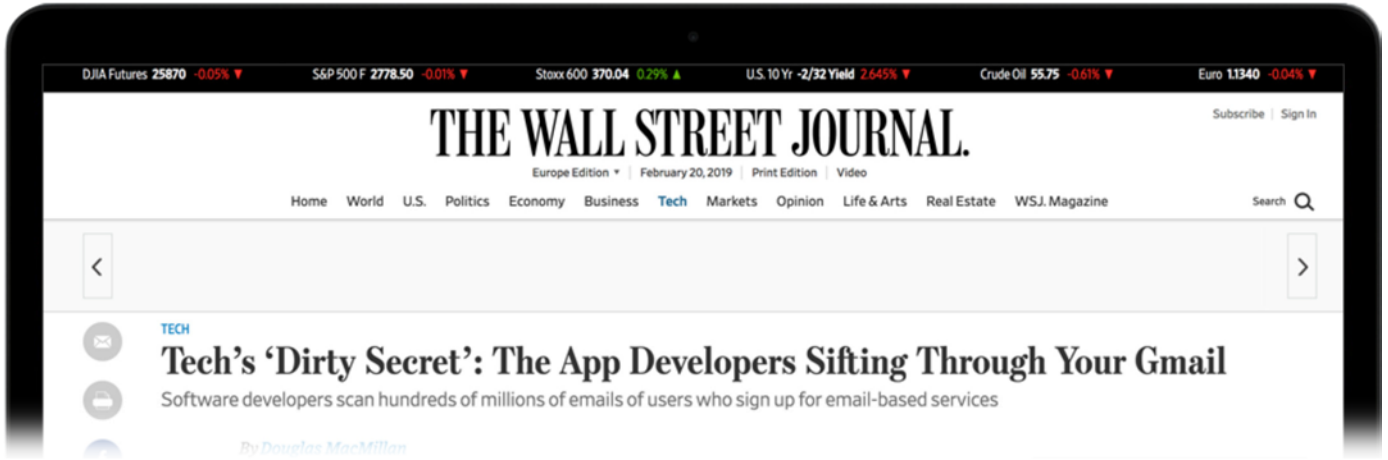
ars TECHNICA

„Brudny sekret" branży technologicznej: twórcy aplikacji przeglądają twojego Gmaila

THE WALL STREET JOURNAL.

Współzałożyciel WhatsAppa Jan Koum odchodzi z Facebooka po sporach związanych z prywatnością danych

THE VERGE



POTENCJAŁ RYNKOWY

USECRYPT

Wykorzystanie oczywistego potencjału rynkowego trzech najdynamiczniej rozwijających się sektorów

	Rynek chmury publicznej		Stacje robocze	Komunikatory	
Globalnie	USD 176 mld	+17.6% CAGR 2017–2021 globalnego rynku chmury publicznej +30.1%	1.4 mld Liczba komputerów osobistych	2.0 bn	+9.4% CAGR 2016–2021 przy założeniu, że liczba użytkowników komunikatorów sięgnie 2,5 mld w roku 2021
Potencjał 12 docelowych krajów	Szacuje się, że rynek oprogramowania do szyfrowania w chmurze osiągnie poziom 5,1 mld USD w 2019 r.	CAGR 2014–2023 globalnego rynku oprogramowania do szyfrowania w chmurze	1,9 mln MŚP oraz 29 mln potencjalnych stacji roboczych	648 mln potencjalnych użytkowników	

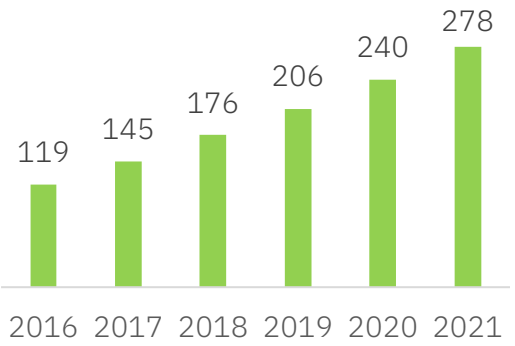
WYKORZYSTANIE CZTERECH ROSNĄCYCH RYNKÓW

USECRYPT

Wykorzystanie czterech dynamicznie rozwijających się rynków: przechowywania danych w chmurze, firmowej poczty elektronicznej, bezpieczeństwa stacji roboczych oraz urządzeń mobilnych

GLOBALNY RYNEK CHMURY PUBLICZNEJ

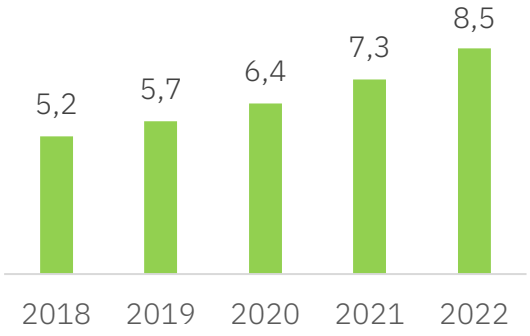
17.6% CAGR



Z prognoz wynika, że rynek chmury publicznej będzie wart 278 mld USD w 2021 r.

RYNEK ARCHIWIZACJI DANYCH

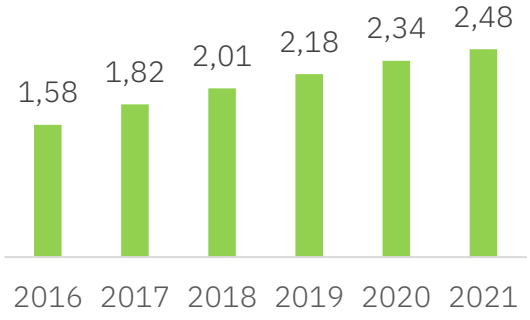
13.1% CAGR



Cały rynek archiwizacji informacji wzrośnie do ponad 8,4 mld USD w 2022 r.

LICZBA UŻYTKOWNIKÓW KOMUNIKATORÓW NA ŚWIECIE

9.6% CAGR



Liczba użytkowników komunikatorów sięgnie niemal 2,5 mld w 2021 r.

RYNEK SZYFROWANIA POCZTY ELEKTRONICZNEJ

23.5% CAGR

Szacuje się, że rynek szyfrowania poczty elektronicznej przekroczy wartość

4.21 mld USD w 2023

Źródło:, Gartner, Radicati Group, Markets and Markets, eMarketer

02

NASZA TECHNOLOGIA I PRODUKTY

CO SPRAWIA, ŻEJESTEŚMY WYJĄTKOWI

USECRYPT

TECHNOLOGIA HVKM

- Technologia Hybrid Virtual Key Management, bazująca na podziale kluczy szyfrujących, stanowi najbezpieczniejszy na rynku sposób wymiany plików oraz wiadomości, oparty na najbardziej zaawansowanych wojskowych protokołach
- Usecrypt jako jedyne rozwiązanie pozwala użytkownikowi na stowrzenie i przechowywanie własnego klucza szyfrującego, którego kluczowy fragment nigdy nie opuszcza stacji roboczej użytkownika
- Rozwiązania konkurencji oparte są o klucze szyfrujące należące do dostawcy oprogramowania, które przechowywane są w chmurze, które przez to są podatne na ataki hackerskie oraz dostęp niepowołanych osób do danych użytkownika

Krytyczna część klucza szyfrującego jest nierozerwalnie związana ze stacją roboczą użytkownika.

„Elementem odróżniającym nas od konkurencji jest HVKM, który gwarantuje, że krytyczny klucz szyfrujący rodzi się i pozostaje nierozerwalnie na stacji roboczej Użytkownika, co gwarantuje, że nie ma technicznej możliwości dostępu do danych użytkownika z poziomu serwera, chmury oraz przez producenta oprogramowania. To zmienia wszystko! Pozostałe rozwiązania przechowują klucze szyfrujące użytkowania na własnej infrastrukturze co czyni je podatnymi na ataki.”

Yuval Rabin, Członek Rady Nadzorczej Usecrypt S.A.

USECRYPTSAFE—KLUCZOWE PRZEWAGI

FUNKCJONALNOŚĆ - KORZYŚĆ

01 **Szyfrowanie lokalnych danych**
Zapobiega utracie i wyciekowi danych w przypadku kradzieży bądź zgubienia stacji roboczej. Rozwiązanie zgodne z RODO.

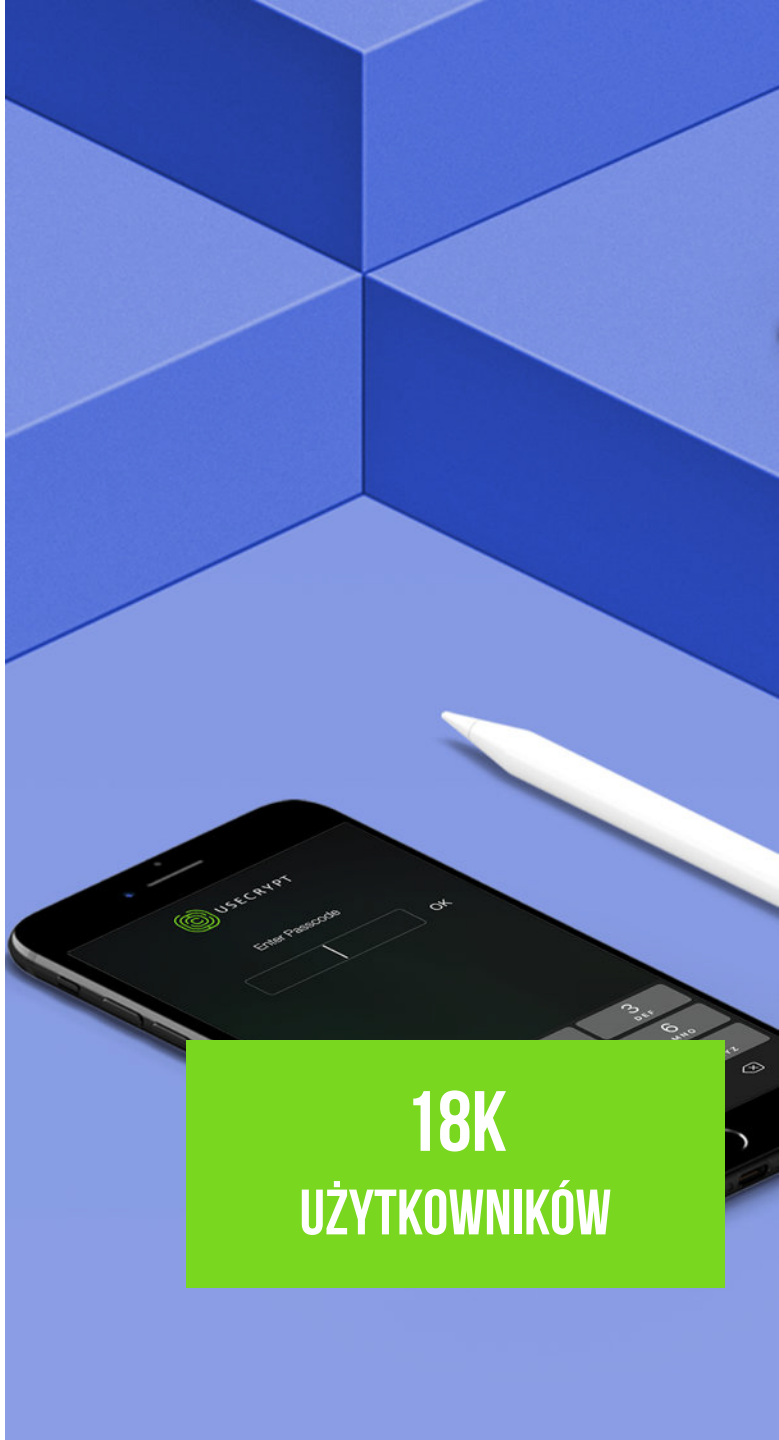
02 **Szyfrowanie danych w chmurze/na serwerze**
Dostawca chmury oraz Usecrypt by-design nidgy nie mają dostępu do Twoich danych

03 **Szyfrowane przesyłanie plików**
Pomiędzy zaufanymi stacjami roboczymi, bez technicznej możliwości dostępu do komunikacji przez niezaufaną trzecią stronę; Brak ograniczeń wielkości załączników

04 **Szyfrowana usługa grupowa**
Dedykowana, szyfrowana przestrzeń dla zaufanych użytkowników

05 **Szyfrowane archiwum i przechowywanie**
Rozwiązanie do tworzenia back-upów

Kluczowe funkcje	Dropbox	BOX	Tresorit	Usecrypt
On-premise (możliwość wdrożenia na infrastrukturze Klienta)	x	x	x	✓
Użytkownik posiada krytyczną część kluczy szyfrujących na własnym urządzeniu	X	x	x	✓
Użytkownicy	500m	41m	n.d.	18k



18K
UŻYTKOWNIKÓW

HVKM—REWOLUCYJNA TECHNOLOGIA

USECRYPT

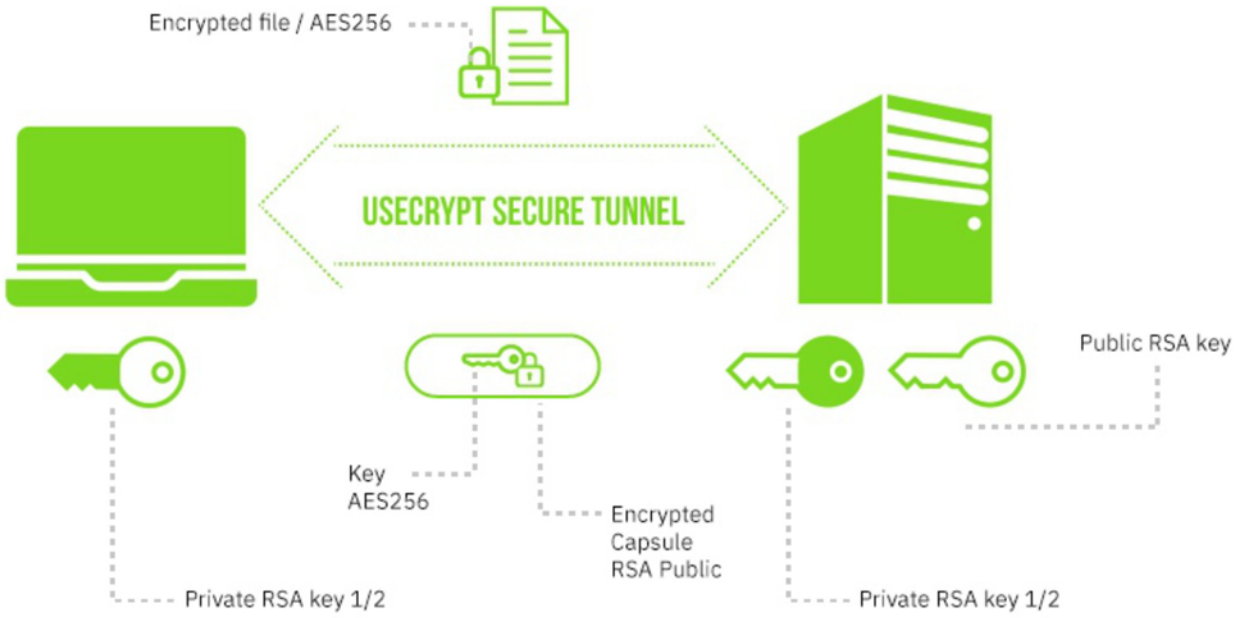
Opatentowana technologia HVKM bazuje na podziale prywatnego klucza szyfrującego, który powstaje na urządzeniu użytkownika i nigdy go nie opuszcza. To właśnie zapewnia pełną ochronę przed nieautoryzowanym dostępem do danych przez trzecią stronę.

Usecrypt Secure Tunnel

- wzmocniany kanał przesyłu danych na serwer, w porównaniu z VPN nasze rozwiązanie jest dedykowane dla apliakcji Usecrypt i uniemożliwia dostęp innym aplikacjom
- w przeciwieństwie do protokołów SSL / TSL, klucze sesyjne generowane są zarówno po stronie urządzenia Klienta jak i na serwerze
- taka konstrukcja nie wymaga stosowania dodatkowego uwierzytelniania (np. w postaci tokenów)

Prywatny klucz

- powstaje i jest związany z jedną, konkretną stacją roboczą, na której powstał
- klucz ma długość 2048bitów (co oznacza odporność na ataki przez kolejne 10 lat



“Półówki” klucza RSA

- Dwie kompletne części
- Każda z nich posiada taką samą moc jak pierwotny klucz
- Wykonanie jakiejkolwiek czynności wymaga sekwencyjnego wykorzystania obydwu „połówek” oraz klucza publicznego

USECRYPT MESSENGER – JEDYNA APLIKACJA, KTÓRA:

01 Szyfruje dane aplikacji na urządzeniu. Brak możliwości wyjęcia treści rozmów oraz wiadomości w przypadku kradzieży lub utraty telefonu.

02 Sprawdza, czy telefon nie został zhackowany. Gwarantuje pewność, że telefon nie nagrywa w tle głośnika oraz mikrofonu podczas rozmowy. Aplikacja nie działa na zhackowanym urządzeniu.

03 Skutecznie usuwa dane. W przypadku gdy Klient jest zmuszony do podania hasła dostępu, specjalny „Panic Code" pozwala na natychmiastowe usunięcie danych aplikacji.

04 Anoninowość IP. Dostawca internetu widzi jedynie IP serwera pośredniczącego. Nigdy nie widzi IP oraz lokalizacji osoby, do której dzwoni Klient.

05 Brak danych na naszym serwerze. Żadne dane nie są przechowywane na serwerze. Usecrypt nigdy nie przekaże danych użytkownika zewnętrznym organom, ponieważ nie przechowuje tych danych.

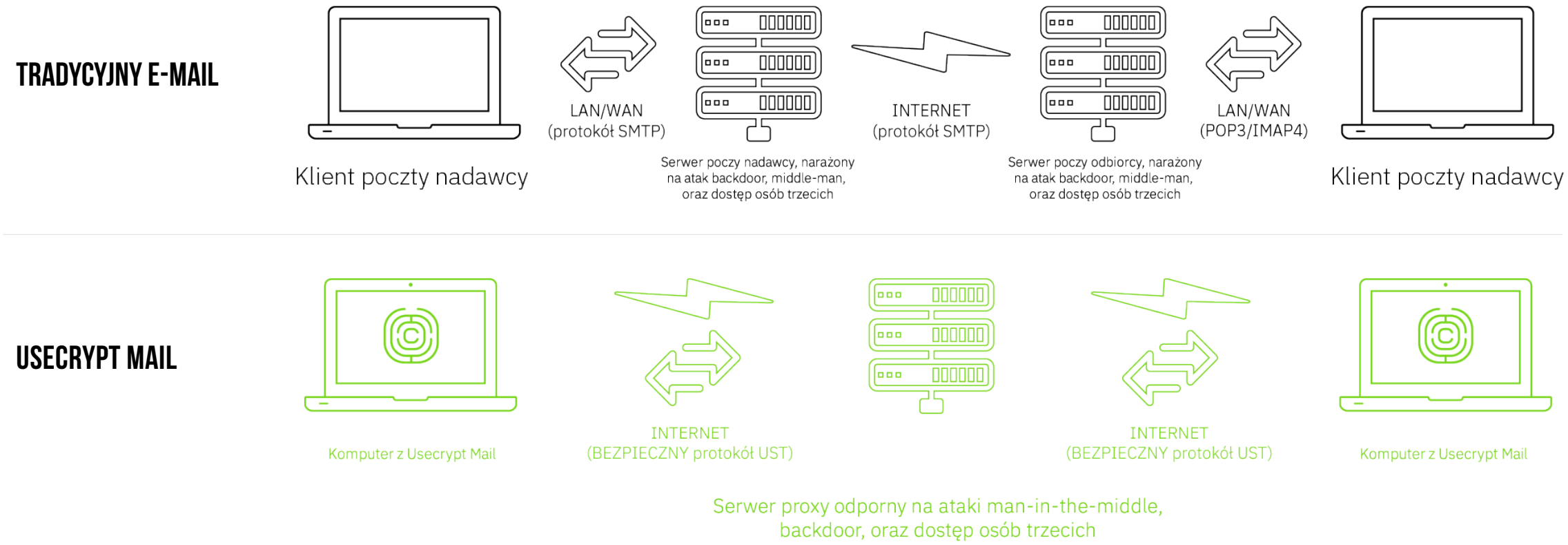
Punkt dostępu	Kluczowe funkcje	WhatsApp	Viber	Telegram	Signal	Usecrypt
Urządzenie	Data-at-rest	x	x	x	x	✓
	Kontrola bezpieczeństwa	x	x	x	x	✓
	Panic code	x	x	x	x	✓
Transmisja	Anonimowość IP	x	x	x	x	✓
Serwer	Brak Meta-danych	x	x	x	x	✓
	Możliwość wdrożenia na infrastrukturze klienta	x	x	x	x	✓
Użytkownicy		1 500m	280m	200m	6m	8k

8K
USERS

USECRYPT MAIL - NASTĘPCA MAILA

USECRYPT

Usecrypt Mail by-design zapobiega dostępowi do danych przez nieuprawnione osoby trzecie (middle-man). Wysyłane i odbierane wiadomości nie przechodzą przez serwery pocztowe, gdzie mogą zostać zhakowane (komunikacja urządzenie do urządzenia).



03 STRATEGIA EKSPANSJI

PLAN EKSPANSJI GLOBALNEJ

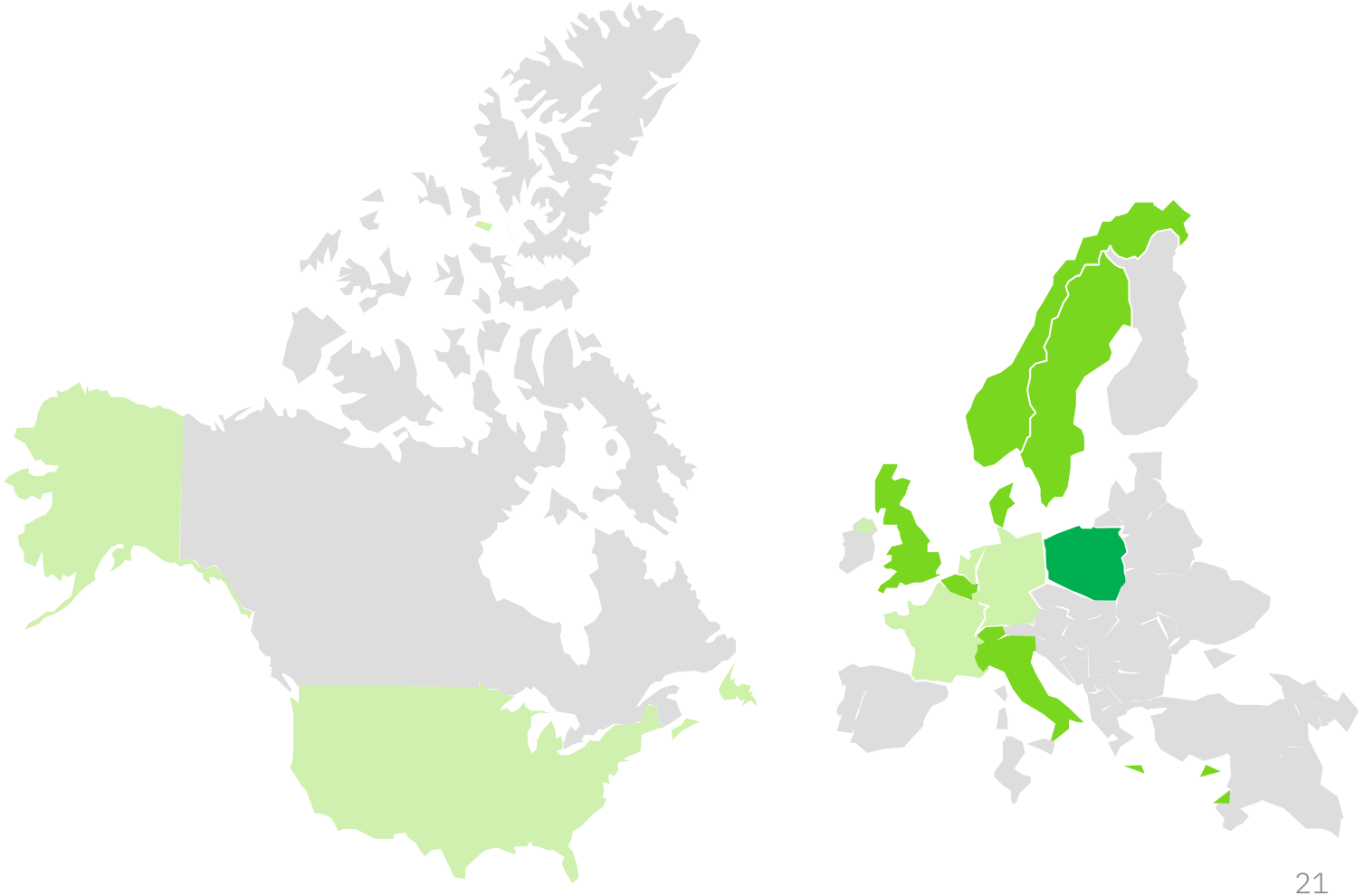
USECRYPT

Wraz z początkiem 2020 r. Usecrypt zamierza prowadzić działalność w 12 krajach na 2 kontynentach – Ameryce Północnej i Europie (oraz w Izraelu).

Firma Usecrypt S.A. działająca w Polsce, baza R&D

Rynki uruchomione/do uruchomienia w 2019r. (Izrael, Cypr, Benelux, Szwajcaria, Monako, Kraje nordyckie, UK)

Rynki do uruchomienia w roku 2020 r. (Francja, Włochy, USA)

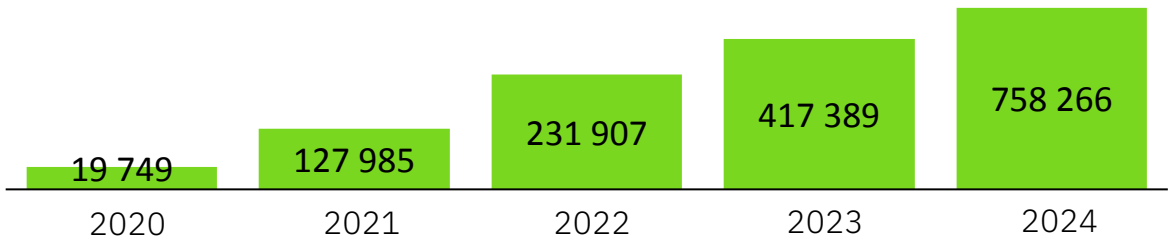


DOMYŚLNA STRATEGIA RYNKOWA DLA 12 KRAJÓW

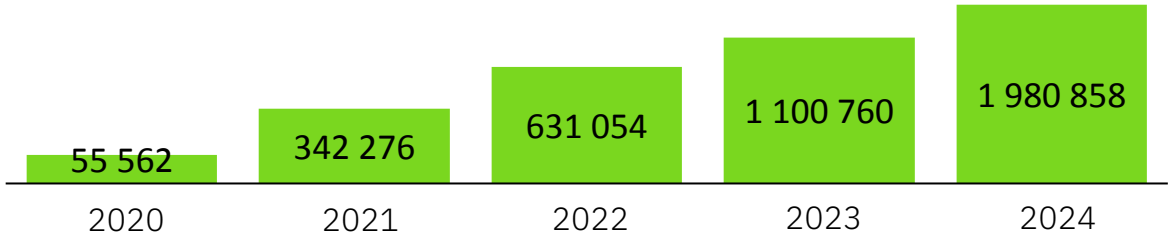
USECRYPT

- Międzynarodowa rozbudowa kanałów sprzedaży oraz powiększenie zespołu ds. sprzedaży
- Budowanie partnerskich kanałów dystrybucji na rynkach docelowych
- Usecrypt zawarł umowy partnerskie w Polsce, Luksemburgu, Szwecji, Norwegii, Izraelu oraz na Cyprze, a obecnie znajduje się w fazie zaawansowanych negocjacji z potencjalnymi partnerami w Niemczech, we Francji i w Monako
- Wykorzystanie kanału internetowego: płatne reklamy, media społecznościowe oraz projekty promocyjne

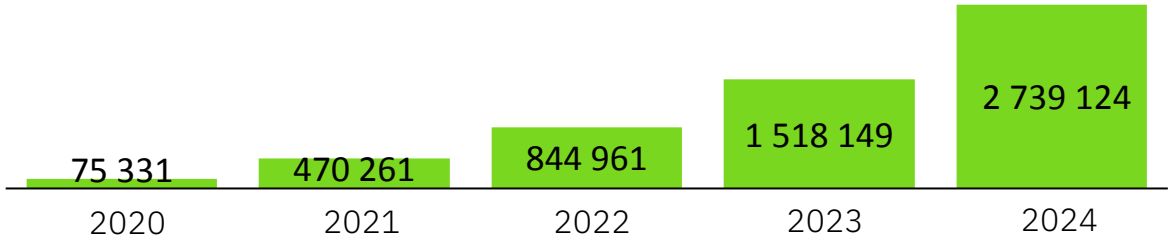
LICZBA UŻYTKOWNIKÓW USECRYPT MESSENGER



LICZBA UŻYTKOWNIKÓW USECRYPT SAFE & MAIL



LICZBA UŻYTKOWNIKÓW ŁĄCZNIE



DANE KONTAKTOWE

USECRYPT

USECRYPT S.A.

adres:
ul. Puławska 2, Plac Unii, Wejście A, 02-566 Warszawa

tel:
+48 22 213 96 44

mail:
bonds@usecrypt.com

MEDIA O NAS:

4 NEW YORK Nasdaq YAHOO! FINANCE HUFFPOST metro

Niniejszy materiał promocyjny jest związany z ofertą publiczną na terytorium Rzeczypospolitej Polskiej („Oferta Publiczna”) obligacji serii F („Obligacje”) spółki pod firmą Usecrypt Spółka Akcyjna z siedzibą w Warszawie („Spółka").

Powyższy materiał ma charakter wyłącznie promocyjny i nie stanowi prospektu emisyjnego ani memorandum informacyjnego w rozumieniu przepisów prawa, w szczególności ustawy z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych (Ustawa o Ofercie) oraz Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2017/1129 dnia 14 czerwca 20va17 r. w sprawie prospektu, który ma być publikowany w związku z ofertą publiczną papierów wartościowych lub dopuszczeniem ich do obrotu na rynku regulowanym oraz uchylenia dyrektywy 2003/71/WE jak również nie stanowi oferty sprzedaży w rozumieniu obowiązujących przepisów prawa ani jakiejkolwiek porady, zachęty, czy rekomendacji.

W związku z ofertą publiczną Obligacji Spółki został opublikowany dokument w rozumieniu art. 7 ust. 8a Ustawy o Ofercie („Dokument”). Oferta publiczna papierów wartościowych następuje w trybie, o którym mowa w art. 7 ust. 8a Ustawy o Ofercie, w związku z tym Emitent nie występował o zatwierdzenie przez Komisję Nadzoru Finansowego Dokumentu. Dokument oraz Warunki Emisji są jedynymi prawnie wiążącymi dokumentami zawierającym informacje o Spółce oraz o Obligacjach Spółki oferowanych na podstawie Dokumentu.

Dokument wraz z ewentualnymi aneksami i komunikatami aktualizującymi, został udostępniony do publicznej wiadomości w formie elektronicznej i jest dostępne na stronie internetowej Spółki https://usecrypt.com

Przed podjęciem jakiejkolwiek decyzji inwestycyjnej inwestorzy powinni uważnie zapoznać się z treścią całego Dokumentu, w tym treścią dokumentów włączonych do Dokumentu przez odniesienie, a w szczególności z ryzykami związanymi z inwestowaniem opisanymi w punktach Dokumentu zatytułowanych „Czynniki ryzyka”. Wszelkie decyzje inwestycyjne dotyczące nabywania obligacji Spółki powinny być podejmowane po analizie treści całego Dokumentu. Każdy inwestor zamieszkały bądź mający siedzibę poza granicami Rzeczypospolitej Polskiej powinien ponadto zapoznać się z przepisami prawa polskiego oraz przepisami praw innych państw, które mogą się do niego stosować.

Odpowiedzialność za sposób wykorzystania. informacji zawartych w niniejszym materiale spoczywa wyłącznie na osobie korzystającej z tego materiału
Oferta publiczna Obligacji jest przeprowadzana na terytorium Rzeczypospolitej Polskiej. Niniejsze materiały promocyjne nie są przeznaczone do publikacji lub dystrybucji poza granicami Rzeczypospolitej Polskiej, w tym w szczególności nie mogą być przekazane lub w jakikolwiek sposób przesłane lub udostępnione na terytorium Stanów Zjednoczonych Ameryki, Kanady, Japonii, Australii ani w jakiejkolwiek innej jurysdykcji, w której stanowiłoby to naruszenie właściwych przepisów prawa lub wymagałoby rejestracji. Ani Dokument ani papiery wartościowe Spółki nim objęte nie zostaną zarejestrowane i zatwierdzone, ani nie będą przedmiotem notyfikacji w jakimkolwiek państwie poza Rzeczpospolitą Polską, w szczególności zgodnie z przepisami prawa dotyczącymi oferowania papierów wartościowych obowiązującymi w Stanach Zjednoczonych Ameryki Północnej. Obligacje oferowane na podstawie Dokumentu nie mogą być oferowane lub sprzedawane poza granicami Rzeczpospolitej Polski.

Materiał promocyjny podlega ochronie wynikającej z ustawy o prawie autorskim i prawach pokrewnych. Powielanie, publikowanie lub jego rozpowszechnianie wymaga pisemnej zgody Emitenta.