USECRYPT – JAK POLSKA TECHNOLOGIA HVKM MOŻE ZMIENIĆ ZASADY KONSTRUKCJI SYSTEMÓW BEZPIECZEŃSTWA

Polska firma Cryptomind oferuje rewolucyjną technologię szyfrowania opartą o mechanizm HVKM, która opiera się na podziale prywatnych kluczy RSA. Wykorzystana w produkcie UseCrypt zapewnia najsilniejsze bezpieczeństwo poprzez eliminację szeregu ryzyk.

Czym jest HVKM?

HVKM (skrót od Hybrid Virtual Key Management) to unikalna metoda szyfrowania wszystkich rodzajów danych cyfrowych w postaci plików. Metoda HVKM posiada certyfikat EUIPO, który potwierdza rejestrację wzorów schematu autorskiej technologii HVKM na 28 państw członkowskich Unii Europejskiej oraz USA.

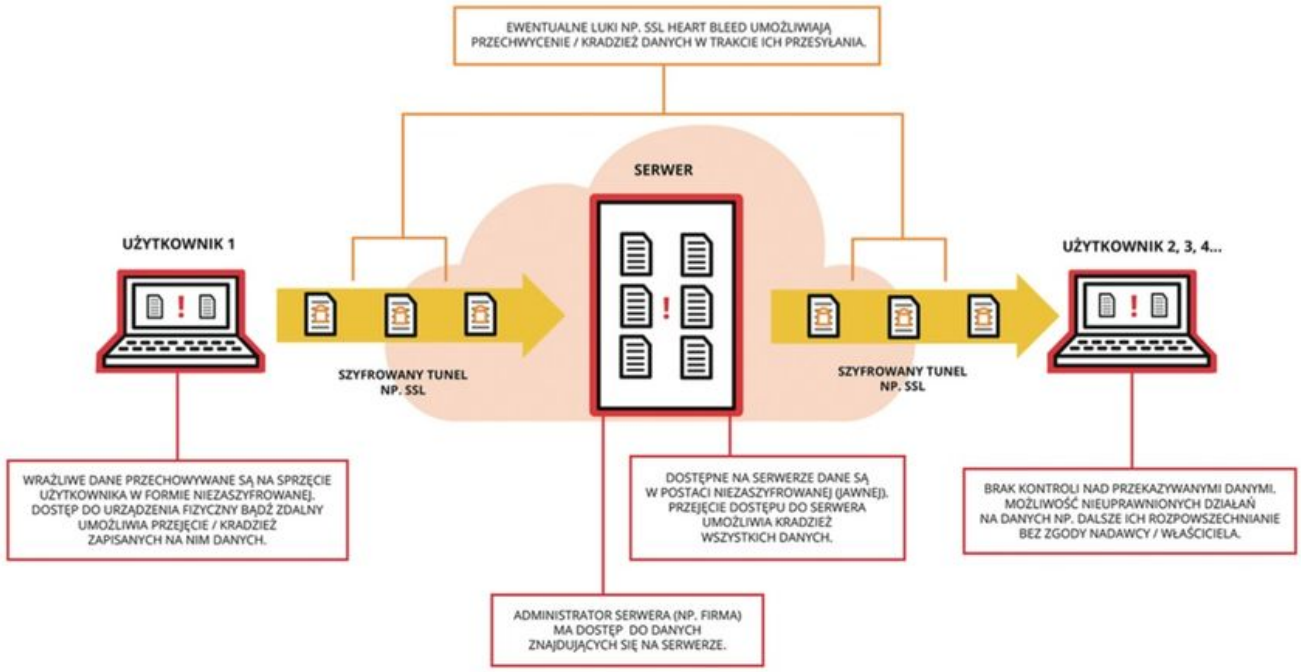
Technologia HVKM polega na kryptograficznym podziale prywatnych kluczy szyfrujących RSA na dwie części. Jedna z nich zawsze znajduje się po stronie urządzenia klienta a druga na serwerze.

Zapewnia to maksymalny poziom bezpieczeństwa przetwarzanych danych jak również gwarantuje zachowanie pełnej poufności przechowywanych w systemie danych. Zaletą takiego podejścia jest to, że kompletny klucz użyty do zaszyfrowania pojedynczego pliku uzyskuje się dopiero gdy jest się w posiadaniu kluczy częściowych (w momencie kontaktu aplikacji z serwerem w trybie on-line). Jedną połowę klucza prywatnego chronioną w autoryzowanym urządzeniu posiada użytkownik, a druga połowa przechowywana i wykorzystywana jest po stronie serwera. Podział kluczy oznacza, że tylko klient posiadający uprawnienia może odszyfrować wyłącznie swoje dane. Producent oprogramowania jak również administrator systemu nie mają technicznej możliwości dostępu do danych klienta, gdyż nie mają dostępu do unikalnej połówki klucza klienta.

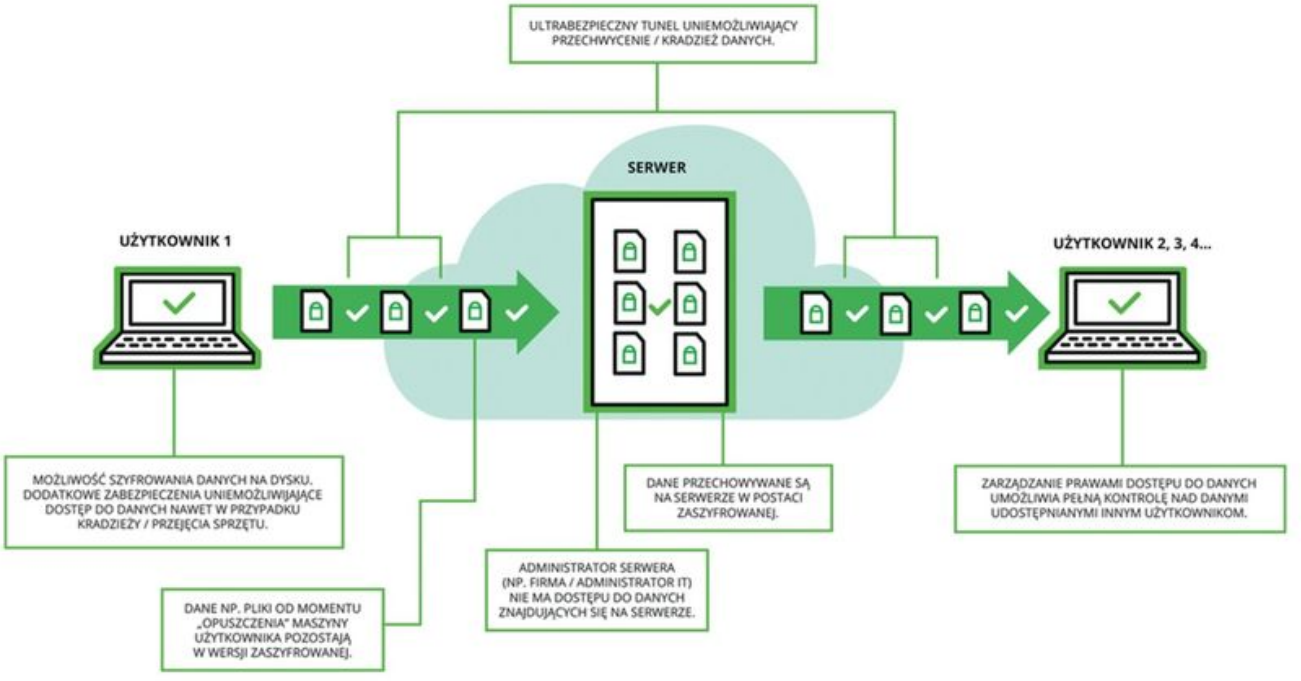
Rozszyfrowanie kluczy symetrycznych AES możliwe jest dopiero po przejęciu obu części klucza RSA. Serwer nie jest w stanie uzyskać dostępu do danych klienta w postaci jawnej (serwer nie posiada, ani nie może wyznaczyć żadnego z prywatnych kluczy kryptograficznych klienta usługi). Klient nie jest w stanie wykonać żadnej operacji kryptograficznej na swoim kluczu prywatnym (podpisu, deszyfrowania) bez udziału serwera. Oznacza to, że samo włamanie na serwer, na którym znajduje się część klucza czy jedynie przejęcie stacji roboczej nie pozwala na dostęp do danych zaszyfrowanych przy użyciu HVKM. Dodatkowo dane na serwerze są replikowane w kilku lokalizacjach, a ich integralność jest stale weryfikowana przez system co chroni je przed fizycznym zniszczeniem. Z kolei w przypadku ewentualnej kradzieży stacji roboczej, dezaktywacja konta odbywa się na podobnej zasadzie jak w przypadku blokady karty kredytowej. Helpdesk aplikacji dostępny jest 24 godziny na dobę.

Poniższe schematy prezentują sytuację gdzie nie stosuję się HVKM i gdzie technologia ta jest

stosowana:



Fot. CryptoMind



Fot. CryptoMind

Jakie zastosowanie ma HVKM?

Autorska technologia HVKM jest wykorzystywana w systemie UseCrypt. UseCrypt Safe to aplikacja, która zapewnia lokalne szyfrowanie danych, bezpieczne ich współdzielenie oraz szyfrowany backup na zewnętrznym serwerze lub infrastrukturze klienta. HVKM jest sercem tej aplikacji, która korzysta z niego na każdym etapie szyfrowania, odszyfrowywania oraz współdzielenia zaszyfrowanych plików.

Czytaj więcej: Szyfrowanie danych sposobem na Ransomware [Cyberdefence24.pl TV]

Jak działa UseCrypt?

Dedykowana aplikacja desktopowa

W przeciwieństwie do wielu innych produktów typu Dropbox, UseCrypt to autorska aplikacja, dzięki czemu wyeliminowane w całości zostały ryzyka związane z pracą poprzez przeglądarkę internetową oraz użytkownik posiada zapewnienie, że dostawca usługi nie będzie miał dostępu do jego danych.

W Dropbox wykorzystywane jest szyfrowanie w modelu „at-rest" oznacza to że dane zostają zaszyfrowane dopiero na serwerze. W trakcie transmisji są chronione wyłącznie poprzez SSL. Nie można jednoznacznie określić w którym momencie dane zostają zaszyfrowane ponieważ definicja „encryption-at-rest" pozwala na jej szeroką interpretację. Model „at-rest" oznacza również brak poufności ponieważ klucze szyfrujące dane pozostają w posiadaniu dostawcy usługi. Powoduje to, że w dowolnym momencie usługodawca może uzyskać dostęp do tych danych.

Czytaj więcej: Dropbox przyznał się w pełni do wycieku po... 4 latach

UseCrypt szyfruje dane już na stacji roboczej, następnie przesyła je w wersji zaszyfrowanej bezpiecznym, autorskim kanałem komunikacji UST. Nikt nie jest w stanie ich odszyfrować i nie ma dostępu do danych klienta.

Szyfrowany kanał komunikacji UST

Po pobraniu i uruchomieniu aplikacji ustanawiany jest szyfrowany kanał komunikacji UST (UseCrypt Secure Tunnel) w oparciu o algorytm uzgadniania klucza metodą Diffiego-Hellmana (określony w standardzie RFC 2631, IEEE 1363-2000 lub ANSI X9.42:2003) co gwarantuje bezpieczeństwo wymiany danych pomiędzy aplikacją, a serwerem.

Generowanie i podział unikalnego klucza szyfrującego

W momencie rejestracji generowane są dwa długie i silne prywatne, losowe klucze **RSA 2048**, w wyniku kryptograficznego podziału na dwie części – opisany wcześniej **HVKM.** Unikalna „połówka" użytkownika przechowywana jest na stacji roboczej, w postaci zaszyfrowanej kluczem **AES256**, podczas gdy druga część znajduje się na serwerze również w wersji zaszyfrowanej, która nigdy nie opuszcza serwera. Podczas pracy użytkownika z aplikacją oba klucze są zawsze odseparowane. Na wypadek utraty stacji roboczej lub zapomnienia hasła użytkownik może wygenerować „recovery key". Recovery key to kopia połówki klucza z urządzenia użytkownika. Wygenerowany jest w postaci pliku, który użytkownik przechowuje na oddzielnym, zewnętrznym urządzeniu, najlepiej w postaci zaszyfrowanej i w bezpiecznym miejscu (np. zdeponowany w sejfie). Każdy recovery key jest dodatkowo zabezpieczony losowo wygenerowanym hasłem jednorazowym, które użytkownik powinien przechowywać w oddzielnym miejscu. Taki proces zabezpiecza dodatkowo recovery key na wypadek jego przejęcia.

Ponadto konfiguracja aplikacji na danym urządzeniu zawiera w sobie parametry konkretnej stacji roboczej, na której UseCrypt jest rejestrowany (**autentykacja konkretnego urządzenia**).

Mechanizm kapsułkowania klucza

Szyfrowanie pliku odbywa się na stacji roboczej użytkownika (stacja robocza musi być w trybie on-line) przy użyciu algorytmu AES256, który generowany jest za pomocą funkcji KDF. Odszyfrowywanie odbywa się dwuetapowo przy użyciu kluczy RSA. Pierwszy etap ma miejsce przy użyciu „połówki"

znajdującej się na serwerze, a drugi na stacji roboczej. Dodatkowo każdy plik zaszyfrowany w UseCrypt jest zaszyfrowany oddzielnym kluczem AES256, a każdy klucz AES zaszyfrowany jest kluczem publicznym RSA.

Współdzielenie zaszyfrowanego pliku polega na stworzeniu zaszyfrowanej kapsułki (**KEM- Key Encapsulation Mechanism**) przechowywanej na serwerze, która powstaje w momencie przesłania do serwera zaszyfrowanego klucza AES pliku. Podczas udostępniania innemu użytkownikowi następnie szyfrowany jest kluczem publicznym RSA odbiorcy, a potem w bezpieczny sposób umieszczany ponownie na serwerze jako zaszyfrowana bezpieczna kapsułka przypisana do wskazanego odbiorcy.

W przypadku, gdy chcemy odebrać użytkownikowi dostęp do pliku, jego kapsułka jest kasowana z serwera i natychmiastowo przestaje on mieć dostęp do pliku czyli nie ma możliwości jego pobrania i odszyfrowania. Jest to dodatkowa przewaga UseCrypt nad standardową pocztą, gdzie w przypadku maila skierowanego do błędnie wybranego odbiorcy nie mamy już możliwości cofnięcia tego procesu i krytyczny załącznik pozostaje w archiwach serwerów pocztowych.

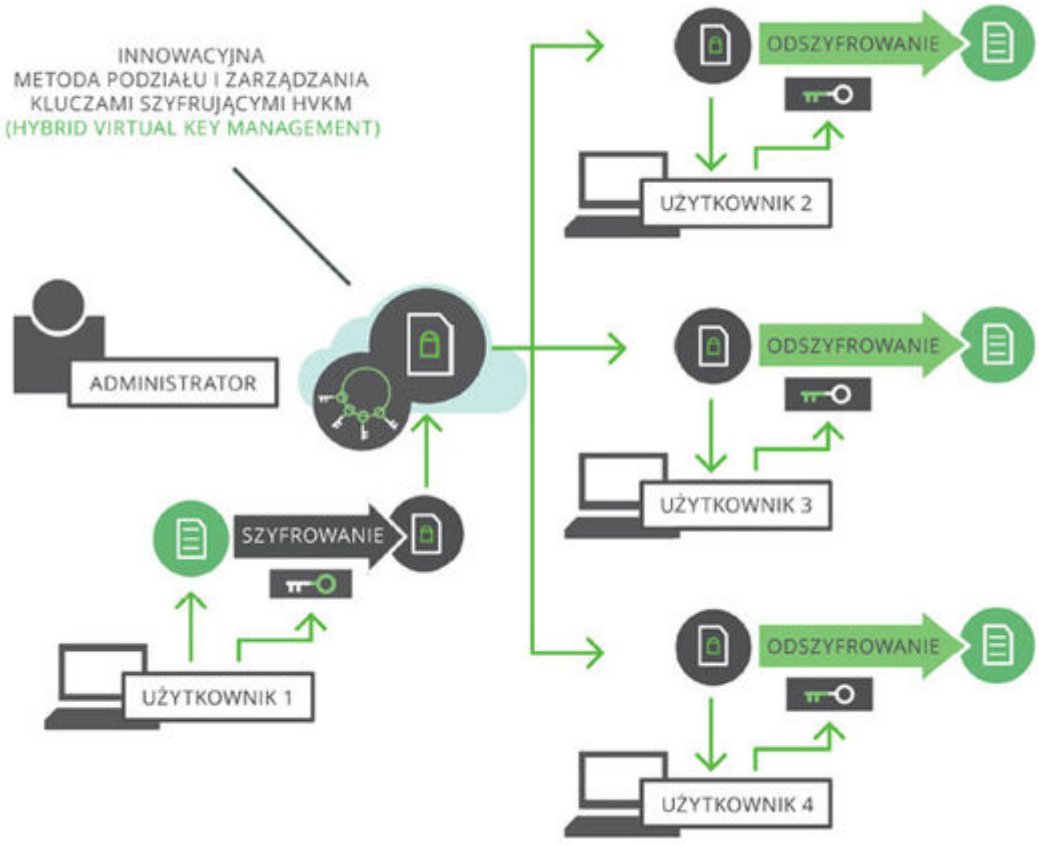
Secure by design

System projektowany jest w ramach tzw. *secure by design*, czyli system w fazie projektu jest tworzony tak, aby był przestrzenią bezpieczną wykluczającą możliwość zewnętrznej ingerencji, ukrycia back-door'ów umożliwiających nieautoryzowany dostęp do zasobów systemu. Zastosowane w rozwiązaniu algorytmy, mechanizmy i użyte protokoły kryptograficzne powodują – według deklaracji producenta – że jest ono odporne na znane metody kryptoanalizy, a sam producent nie ma technicznej możliwości dostępu do danych klientów.

Korzyści dla Dyrektorów IT

Oprogramowanie klienckie systemu może być instalowane na komputerach oraz smartfonach z systemem operacyjnym: Windows, Android, iOS oraz Mac OS. System UseCrypt posiada funkcjonalność pozwalająca na przyznawanie uprawnień dostępu na poziomie plików oraz folderów za pomocą mechanizmu zarządzania uprawnieniami, które przydzielane są przez właściciela danego dokumentu w ramach wdrożonej polityki. UseCrypt nie integruje się z usługami katalogowymi. Cryptomind wychodzi z założenia, że integrowanie jego rozwiązania z innym narzędziem typu active directory opartym na Lightweight Directory Access Protocol (LDAP) może być związane z propagowaniem dodatkowych podatności i wykorzystaniem tych usług do przejęcia danych. Znane są ataki, które są oparte o podatności Active Directory. Kolejnym etapem rozwoju systemu będzie wdrożenie UseCrypt API, które będzie umożliwiało integrację z systemami zewnętrznymi takimi jak obiegi dokumentów lub rejestratory pism kancelaryjnych i podnosząc poziom bezpieczeństwa tych systemów.

System umożliwia gradację poziomów uprawnień, z wykorzystaniem których można wykreować kilka poziomu dostępu użytkowników w prosty i bezpieczny sposób. Nadane uprawnienia mogą mieć uporządkowaną, hierarchiczną strukturę, która można być dowolnie rozbudowywana.



Fot. CryptoMind

Właściciel danych znajduje się na szczycie hierarchii, a poniżej umiejscowieni są operatorzy, którzy mogą nadawać uprawnienia dotyczące konkretnych danych. Ponadto każda operacja wykonana przez użytkownika potwierdzana jest złożeniem podpisu cyfrowego, co pozwala na wyeliminowanie sytuacji, w której użytkownik zaprzecza wykonaniu określonej czynności w systemie.

UseCrypt zmienia sytuację dyrektorów IT, szefów bezpieczeństwa i administratorów. W systemach, w których rozwiązanie to nie jest stosowane, dyrektor IT ma dostęp do wszystkich danych firmy. Zastosowanie UseCrypt powoduje, że dyrektor IT nie ma technicznej możliwości podglądu danych szyfrowanych przez pracowników. Oznacza to, że ewentualny atak na jego konto nie daje technicznej możliwości dostępu do zasobów całej firmy. Powoduje to, że pracownicy działów IT przestają być głównym celem ataków skierowanych na uzyskanie dostępu do wrażliwych danych.

Wszystko to powoduje, że UseCrypt stanowi istotny nowy element konstrukcji systemów bezpieczeństwa, który poza korzyściami dla Dyrektorów IT daje również korzyści dla całej organizacji, czyniąc wymianę i przechowywanie plików znacznie bezpieczniejszą.

Czytaj więcej: Prezes i dyrektor IT w firmie różnie oceniają cyberbezpieczeństwo

Artykuł powstał na postawie materiałów dostarczonych przez firmę CryptoMind.