CryptoPanel

edycja #7

...And Microsoft For All...

Bezpieczeństwo danych w Microsoft365 to przede wszystkim ich szyfrowanie. Poprawna implementacja Double Key Encryption (DKE) - przykład strategii Hold Your Own Key (HYOK).

CryptoPanel

dziś dyskutują

Joanna Rzepka

Channel Sales Manager
Joanna.Rzepka@thalesgroup.com
mob. +48 600 537 666

Jarosław Ulczok

Pre-sales Consultant
Jaroslaw.Ulczok@thalesgroup.com
mob. +48 603 056 667


...AND
MICROSOFT
FOR ALL
CBS
SONY
COMPACT
disc
DIGITAL AUDIO
25DP 5178
STEREO
JASRAC
PRODUCED BY METALLICA WITH FLEMMING RASMUSSEN ENGINEERED BY FLEMMING RASMUSSEN
MIXED BY STEVE THOMPSON AND MICHAEL BARBIERO
"THE PRINCE" Not produced. Engineered by Mike Clink and Toby 'Rage' Wright.
Rough mix by Flemming Rasmussen.
©1988 METALLICA
MS ADCA 5:00
MS SQL EKM 10:01
AZURE BYOK 21:05
W11 & TPM 22:30
O365 DKE 6:20
CDN... 3:20
ALL RIGHTS OF THE MANUFACTURER AND OF THE OWNER OF THE RECORDED WORK RESERVED UNAUTHORIZED PUBLIC PERFORMANCE, BROADCASTING AND COPYING OF THIS DISC PROHIBITED. CBS/SONY RECORDS, A DIVISION OF CBS/SONY GROUP INC. TOKYO JAPAN

CryptoPanel

problem

co nas boli...

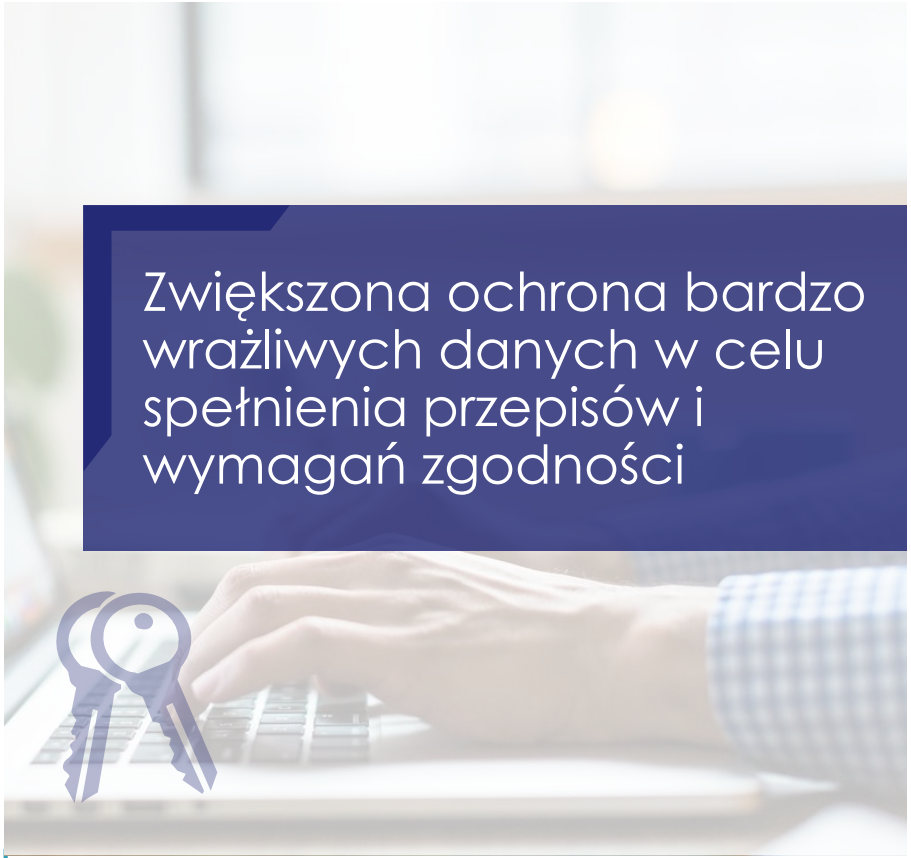
- Nasza organizacja składa się z konglomeratu firm (spółki zależne, spółki „córki”, itp.).
- Korzystamy szeroko z rozwiązań firmy Microsoft.
  - W tym z Microsoft 365
- Słyszeliśmy o DKE ale nie wiemy jak wdrożyć to rozwiązanie w sposób poprawny i bezpieczny.

- Ja zapewnić poufność dla części dokumentów Office?
- Czy stosując DKE możemy wymieniać dokumenty zaszyfrowane z firmami w ramach grupy i spoza niej?
- Czy warto zakupić *Key Broker Service* dla obsługi DKE czy utrzymywać go samemu?
- Czy DKE nie będzie wąskim gardłem przy obróbce dokumentów

CryptoPanel

rozwiązanie

Zacznijmy od początku. Czym jest Double Key Encryption (DKE)?



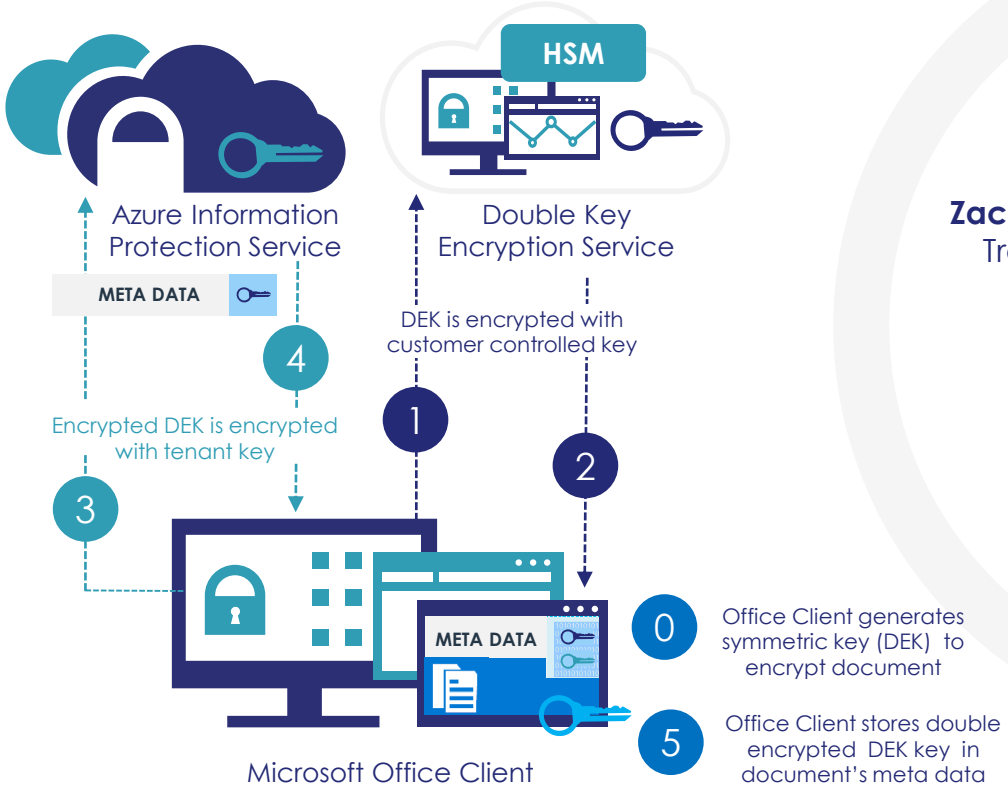
Chroni dane dwoma kluczami. Aby uzyskać dostęp do zawartości, musisz posiadać oba klucze: klucz kontrolowany przez klienta i klucz klienta w Microsoft Azure

Brak dostępu osób trzecich. Ponieważ jeden klucz jest zawsze pod Twoją kontrolą, Microsoft nigdy nie ma dostępu do Twoich danych

Spójne środowisko użytkownika. Ujednolicone środowisko etykietowania w całym repozytorium danych, zarówno dla administratorów i użytkowników

THALES

DKE – proces szyfrowania



Zachowaj kontrolę nad swoimi danymi
Treść jest szyfrowana kluczem klienta przed przesłaniem do Azure

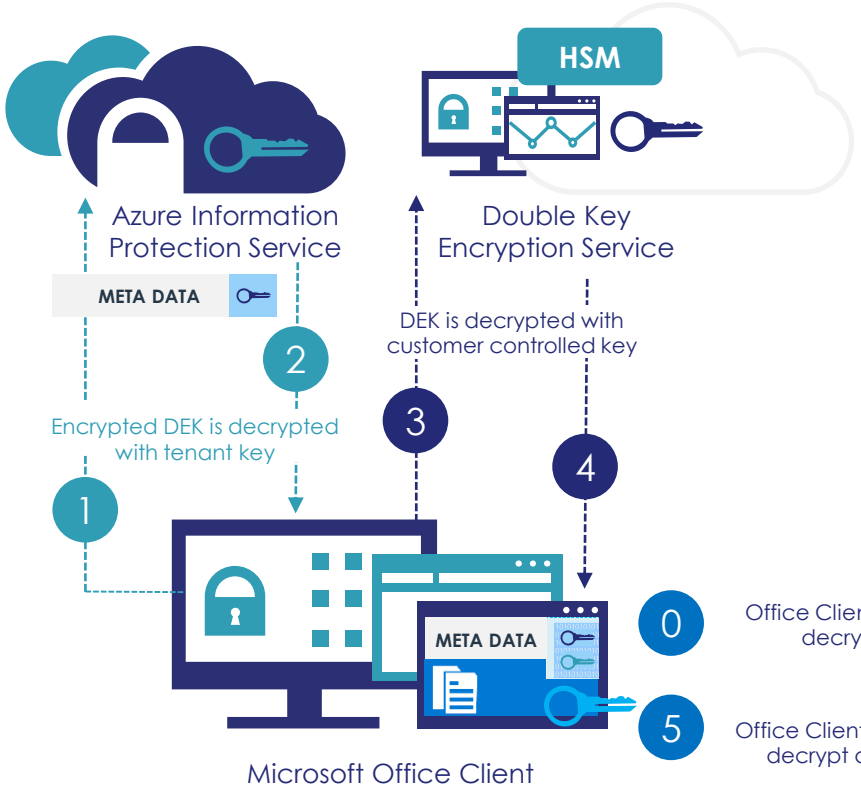
Klucze szyfrowania

- Klucz klienta w Azure
- Klucz klienta w usłudze Double Key Encryption (DKE)

DEK – data encryption key

THALES

DKE – proces deszyfrowania



Office Client request to decrypt DEK

Office Client uses DEK do decrypt document

DEK – data encryption key

Zachowaj kontrolę nad swoimi danymi
Dane nigdy nie są w postaci jawnej na platformie Azure, dzięki czemu są niedostępne dla firmy Microsoft

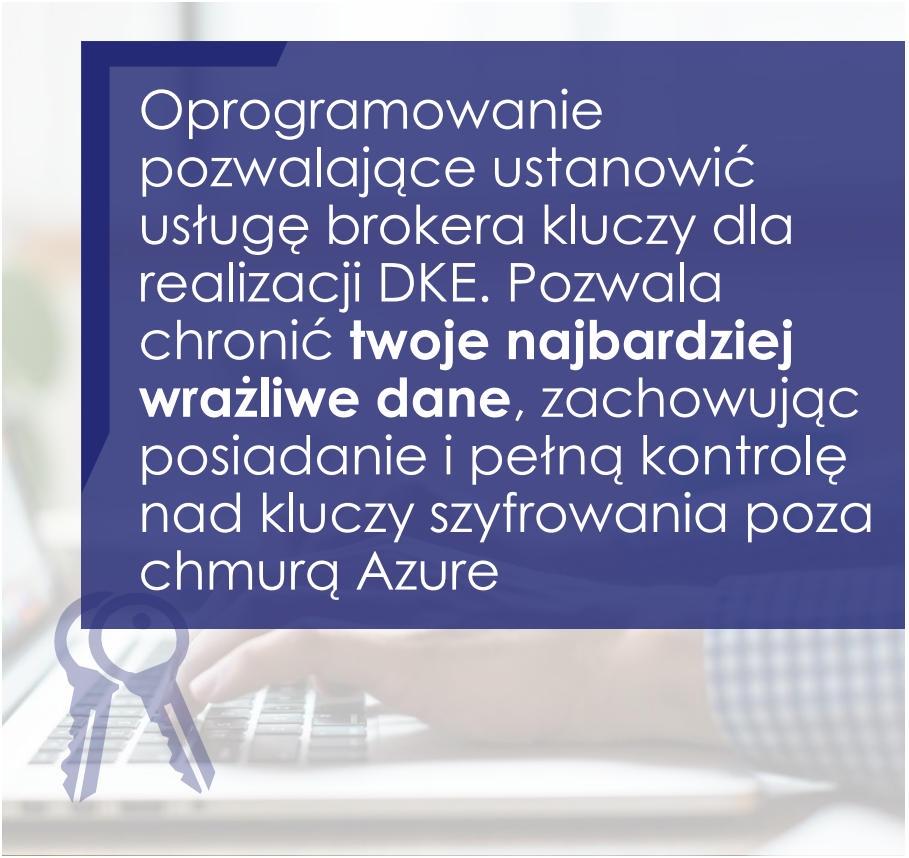
Klucze szyfrowania

Klucz klienta w Azure

Klucz klienta w usłudze Double Key Encryption (DKE)

THALES

A czym jest Luna Key Broker for Microsoft DKE?



Oprogramowanie pozwalające ustanowić usługę brokera kluczy dla realizacji DKE. Pozwala chronić **twoje najbardziej wrażliwe dane**, zachowując posiadanie i pełną kontrolę nad kluczy szyfrowania poza chmurą Azure

Rozszerzona kontrola nad danymi i kluczami

Generuje klucze szyfrowania i zarządza nimi zgodnie z zasadami bezpieczeństwa, zachowując wyłączną kontrolę nad danymi prze użytkownika

Elastyczne wdrażanie

Luna Key Broker dla Microsoft DKE można wdrożyć w chmurze lub lokalnie

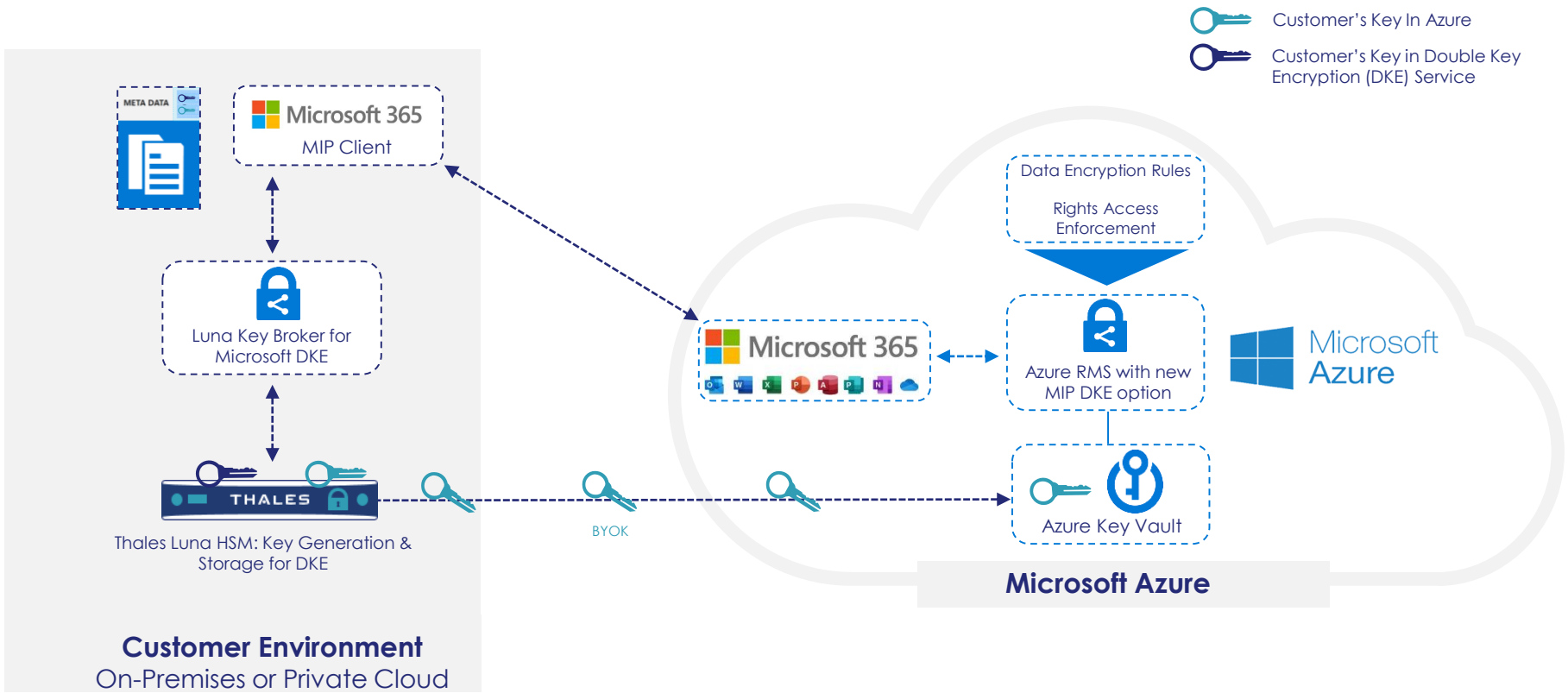
Bezpieczeństwo i zgodność

Pomaga spełnić wewnętrzne regulacje i wymogi dotyczące zgodności, takie jak RODO, HIPAA i Schrems II

Klucze przechowywane przez klienta są utrzymywane w innym miejscu niż znajdują się Twoje poufne dane. Dzięki generowaniu, zarządzaniu i przechowywaniu kluczy szyfrowania w module HSM Luna z certyfikatem FIPS 140-2 Level 3

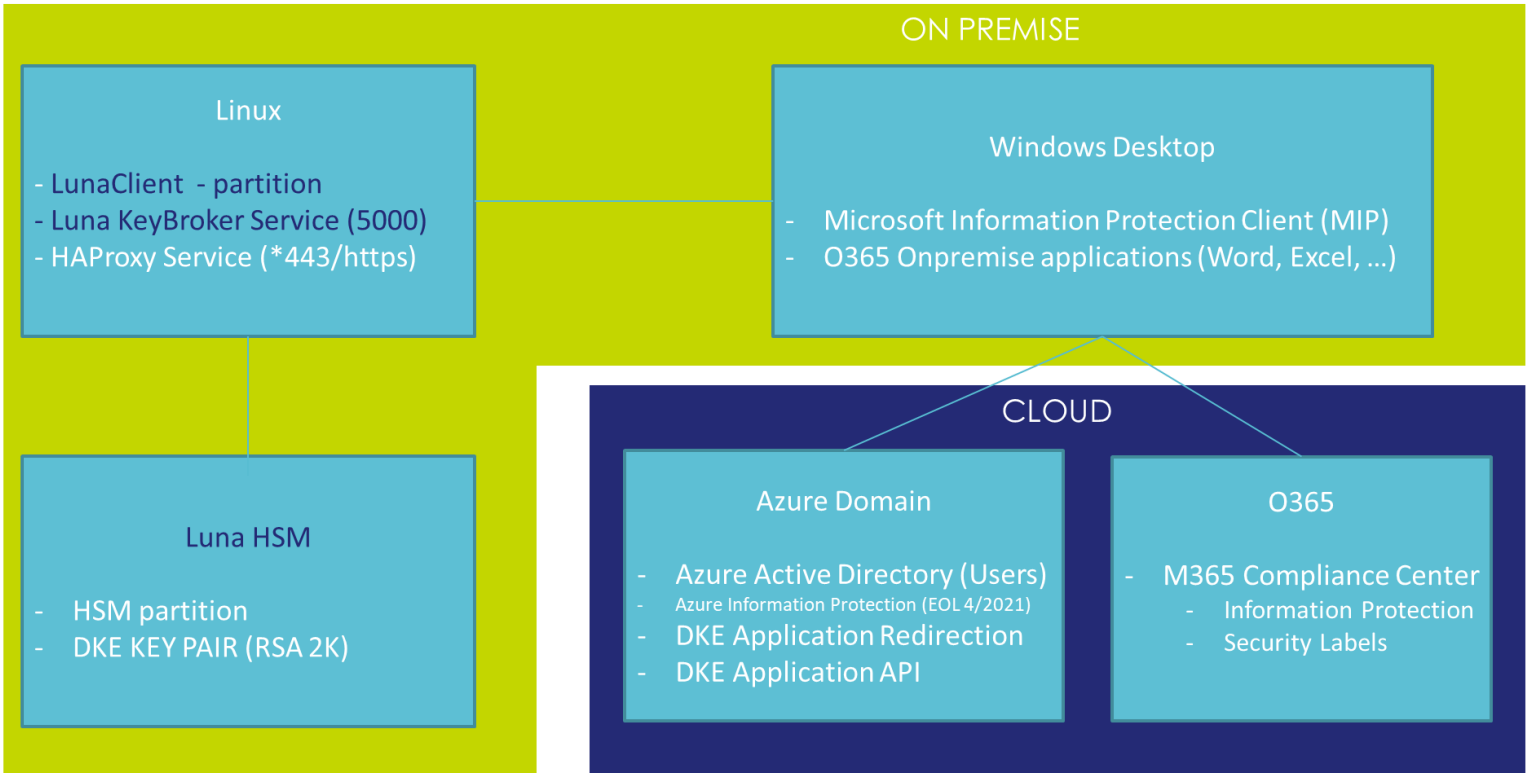
THALES

Microsoft 365 Encryption with Luna Key Broker for Microsoft DKE



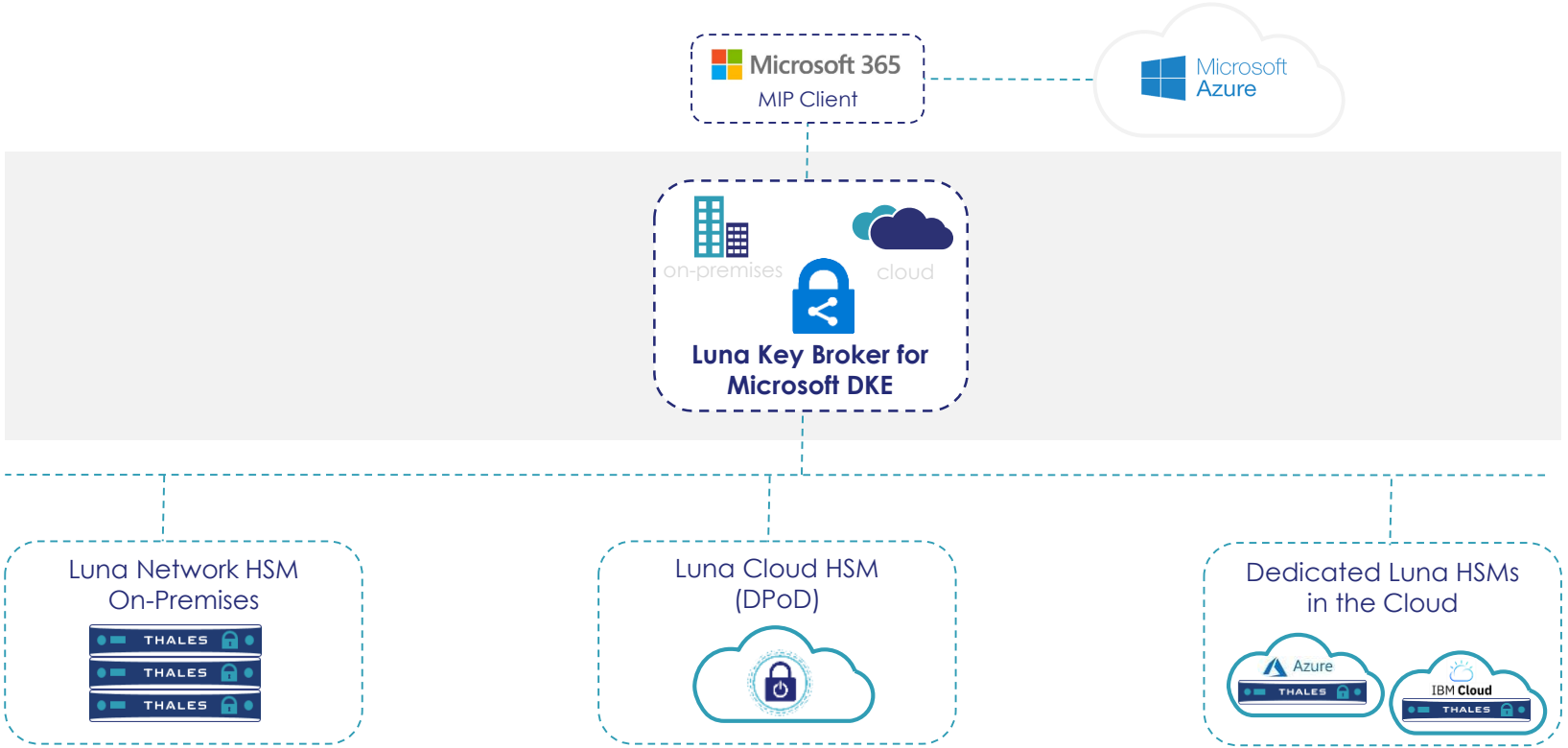
Przykład uruchomienia

Deployment - Luna KeyBroker - example



THALES

Luna Key Broker for Microsoft DKE Deployment Options



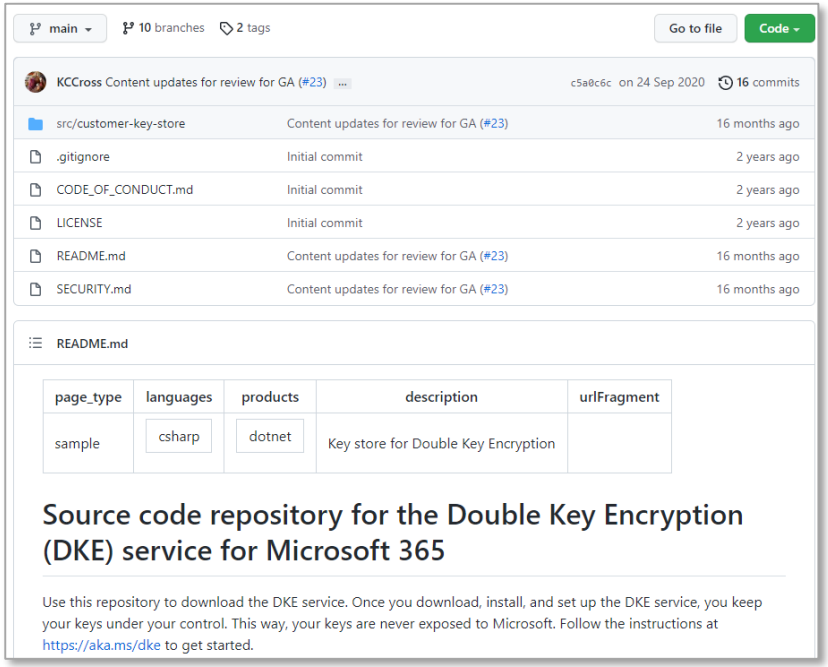
THALES

Dlaczego Key Broker z Thales? A może „dziergać” samemu?

Oczywiście można wdrożyć usługę Key Broker samodzielnie…

Microsoft podaje działający przykład

- GitHub: https://github.com/Azure-Samples/DoubleKeyEncryptionService
- Wideo poradnik: https://www.youtube.com/watch?v=vDWfHN_kygg



No, niby wszystko jest ale…

- Jak przechowywane są klucze dla ochrony twoich wrażliwych danych?
- Kto odpowiada za utrzymanie i wsparcie rozwiązania?

THALES

Dlaczego Key Broker z Thales? A może „dziergać samemu”?

W notatce do źródeł DKE by MS jest taki zapis:

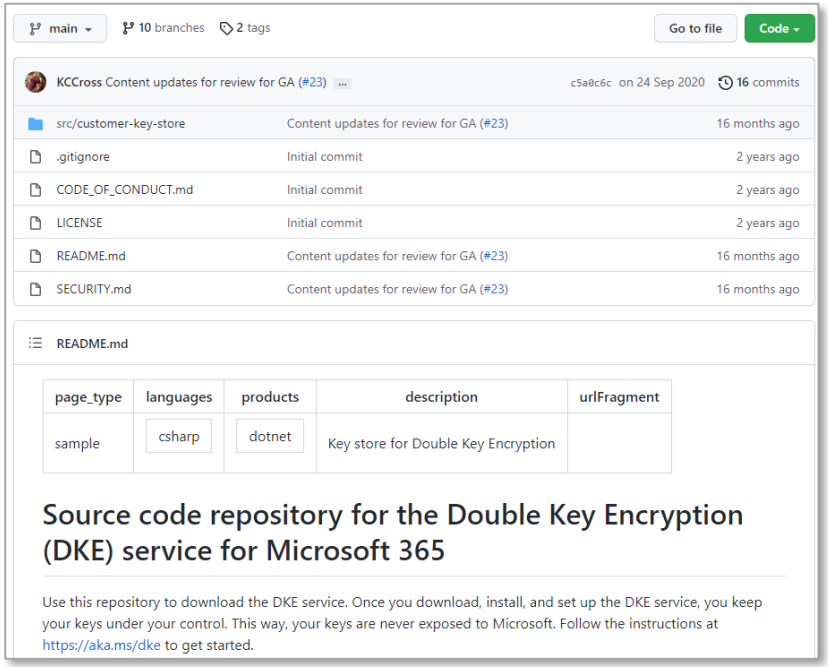
IMPORTANT NOTICE: This project includes code for encryption libraries. You are responsible for complying with all applicable international and national laws that apply to this software, including the U.S. Export Administration Regulations, as well as end-user, end use and destination restrictions by U.S. and other governments.

(Azure-Samples/DoubleKeyEncryptionService: Download, install, and set up the Double Key Encryption service for Microsoft 365. (github.com))

Dla odmiany w official anouncement dla DKE jest taki zapis:

In addition Microsoft has partnered with Thales to manage the keys in your organization’s control by using a Thales Luna HSM, which you own, control and meets FIPS 140-2 Level 3 high assurance NIST standard. Please read more about this powerful integration here.

(Announcing new Microsoft Information Protection capabilities to know and protect your sensitive data - Microsoft Tech Community)



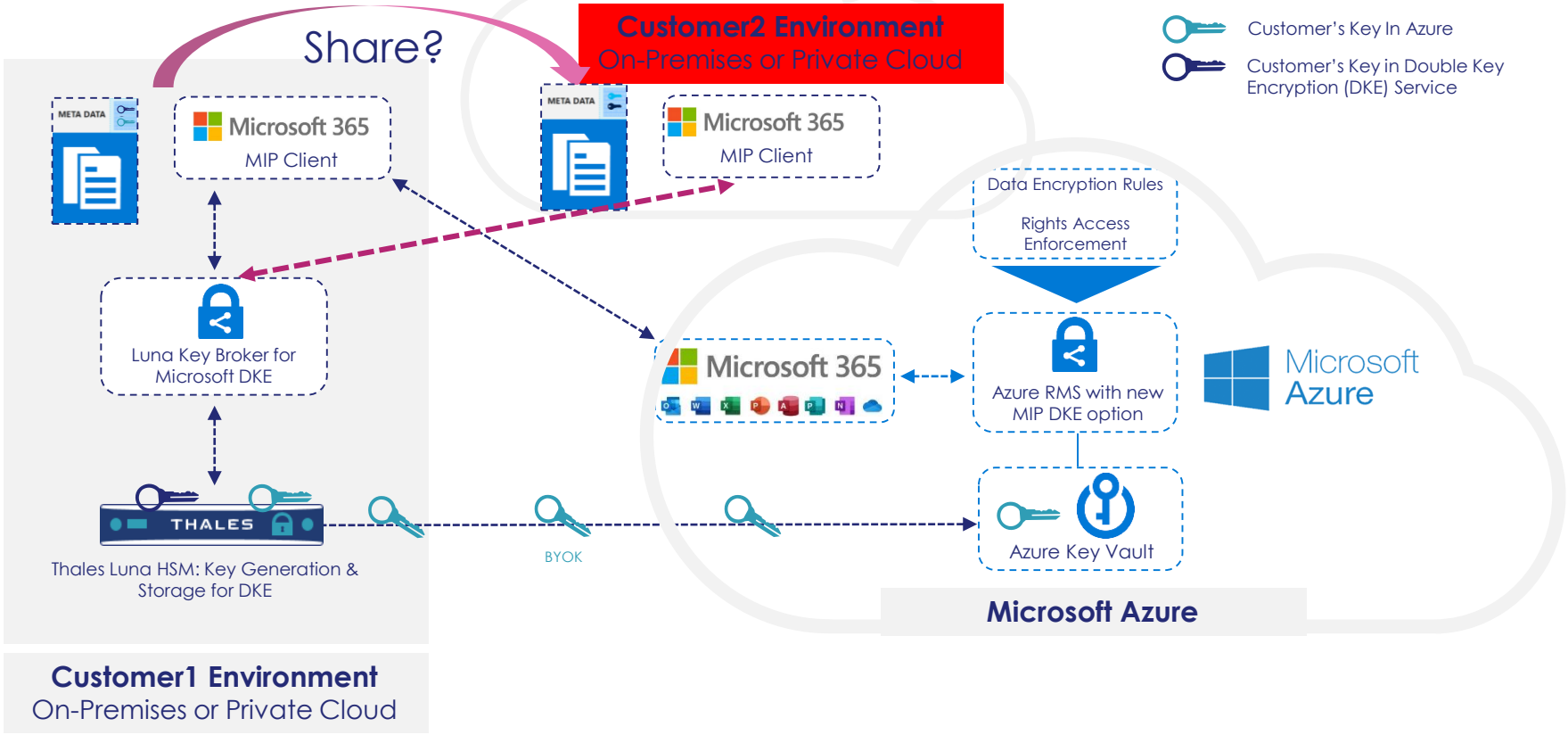
THALES

Dlaczego: Luna Key Broker for Microsoft DKE?

- **Opracowane, rozwijane i utrzymywane przez Thales**
- **Chroni klucze za pomocą modułów Luna HSM**
  - Pojedyncze urządzenie, grupa HA, Luna Cloud HSM
- **Pozwala wdrożyć klaster**
  - Dowolna liczba węzłów dla zwiększenia dostępności
- **Wiele kluczy dla różnych grup użytkowników**
  - Wiele etykiet wrażliwości, każda z własnym kluczem
- **Wymiana kluczy (rollover)**
- **…**

THALES

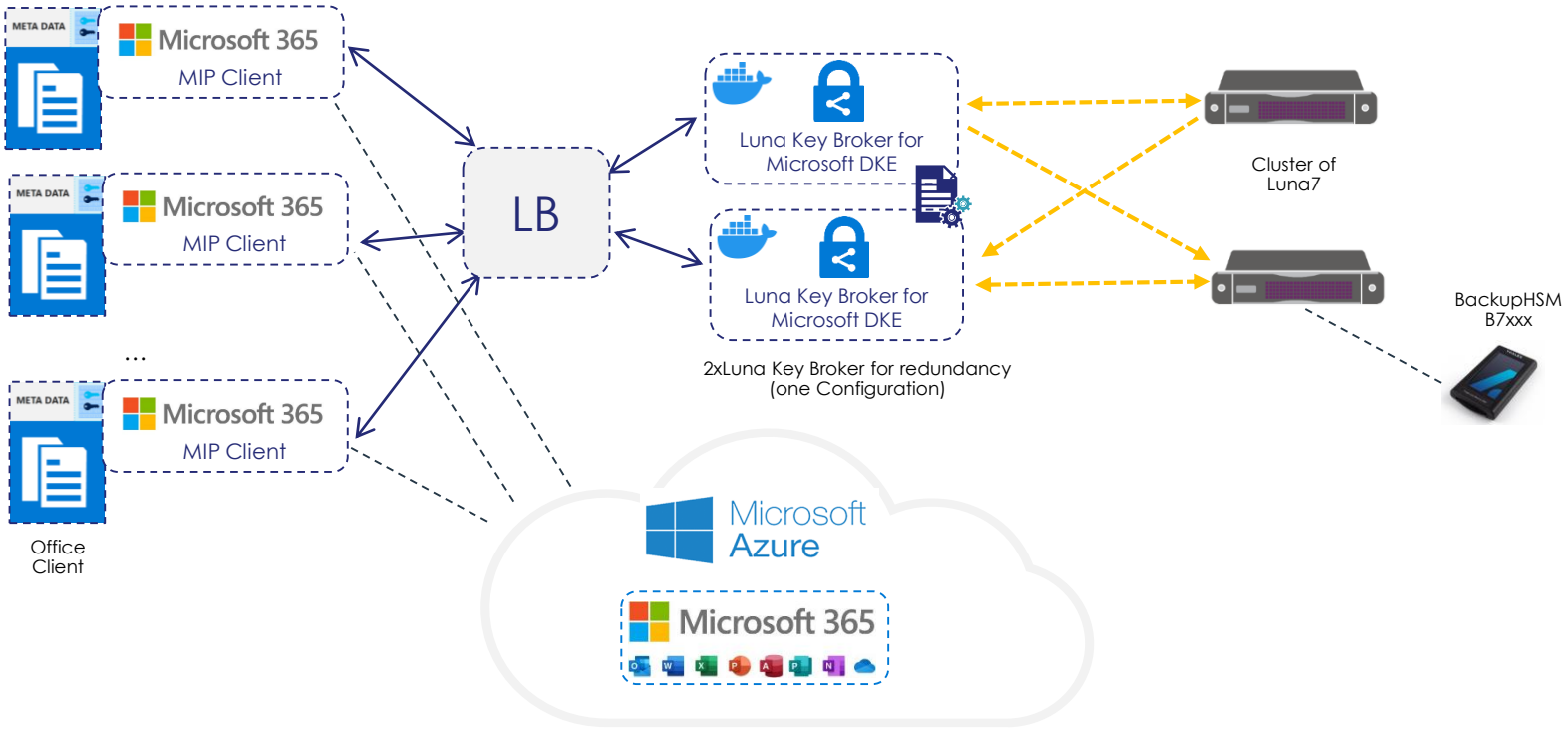
A jak z dzieleniem dokumentów w grupie firm?



CryptoPanel

podsumowanie

Problem i propozycja rozwiązania



I słowo o tym „*co potrzeba*”?

- **Luna7 szybko i łatwo integruje się z Luna Key Broker**
- **Dla wymagających:**
  - Możliwość wdrożenia klastra HA/LB oraz
  - Kopia kluczy na wypadek DR (BackupHSM B7xx lub DPoD)

- **produkty dostępne w kanale partnerskim**
- **licencja dożywotnia lub subskrypcja**
- **licencja demo do testów**

BOM:

- **2x Luna A700 – 2x 18k €**
- **1x Luna Key Broker - 1x 7k €**
- **0x Luna Client License!**
- **1x Luna Backup HSM B700 – 1x 6k €**

Jak licencjonowany jest Luna Key Broker for DKE?

License is *per Key Broker* ***Configuration***

- Licencja umożliwia wdrożenie dowolnej ilości instancji dla redundancji lub zwiększenia wydajności (np. wdrożone jako kontenery)
- Tylko jedna konfiguracja jest możliwa(tj. zestaw użytkowników/kluczy)
- Dodatkowe konfiguracje oznaczają dodatkową licencję
- Obowiązkowa opieka (wraz z innymi komponentami Luna HSM)

Part Number	Description
908-000468-001	LUNA KEY BROKER FOR MICROSOFT DKE

THALES

Definicja „Configuration”

Zasada#1: Zapytaj swojego zaufanego SE ;-)

Problem: Zależy w dużej mierze od konfiguracji klienta

Technicznie rzecz biorąc, wdrożenie (= zliczone konfiguracje) składa się z 2 części:

- Konfiguracja kontenera, np. ***docker-compose.yml***
- Konfiguracja modułu HSM np. **Chrystoki.conf** (+certyfikaty)

THALES

„Nauczki” i tego nie znajdziecie w dokumentacji

Do we have a list of URI called by Azure AIP client to DKE service?

- the two URI's are:
  - https://<host>/<pubkey>
  - https://<host>/<pubkey>/<ID>/decrypt

Czy DKE Key Broker można wdrożyć bez HSM-a?

- tak, ale czy to jest poważne?

Czy każdy Micorosoft365 może korzystać z DKE?

- *Double Key Encryption for Microsoft 365 comes with Office 365* ***E5*** *or Microsoft 365* ***E5****.*

Czym różni się DKE od HYOK?

- ?... *Będzie* na kartkówce ☺
- *Double Key Encryption encrypts your data* ***with two keys.*** *Your encryption key is* ***in your control*** *and the second key is stored in Microsoft Azure, allowing you to move your encrypted data to the cloud. HYOK protects your content* ***with only one key*** *and the* ***key is always on premises****.*

Czy dla integracji Luna Key Broker for Microsoft DKE z Luna HSM potrzebuję licencji na Luna Client?

- Nie! ☺ Prezent od Thales-a

Jak dokładnie przebieg proces szyfrowania/deszyfrowani dokumentu i pobierania kluczy?

- Wyjaśnia to ten film: https://youtu.be/0d-A4OYxaEA?t=350

THALES

Materiały

Oprogramowanie do pobrania lub wersja ewaluacyjna...

- Bardzo prosimy o kontakt z nami!

Dokumentacja:

- **Luna7**: https://www.thalesdocs.com/gphsm/luna/7/docs/network/Content/Home_Luna.htm
- Podręcznik Integracji **Luna Key Broker**: https://cpl.thalesgroup.com/resources/encryption/luna-key-broker-for-microsoft-double-key-encryption-solution-brief

Zapraszamy także do obejrzenia:

- Jak przebiega szyfrowania i deszyfrowanie DKE: https://youtu.be/0d-A4OYxaEA?t=350

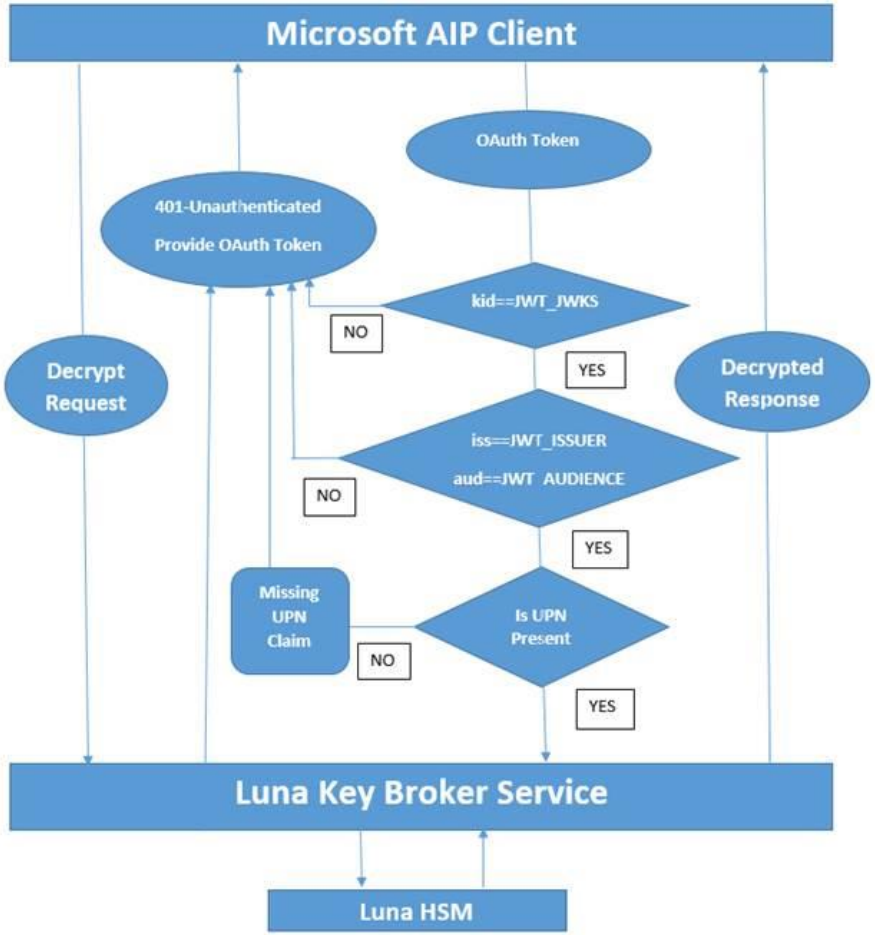
Polecamy DKE FAQ:

- https://docs.microsoft.com/en-us/microsoft-365/compliance/double-key-encryption-overview?view=o365-worldwide

THALES

CryptoPanel

Authentication flow



Cryptographic Performance of HSMs

Operation	Key-Size	CipherText-Size	Ops/sec 2xA700	Ops/sec 2xA750	Ops/sec 2xA790
Decrypt	RSA-2048	16	2.000	9.900	20.000
	RSA-3072	16	630	3.200	6.200
	RSA-4096	16	270	1.400	2.700
	RSA-8192	16	2	1 2	24