MAINFRAME CRYPTO

Crypto Performance

Greg Boyd

gregboyd@mainframecrypto.com

May 2023

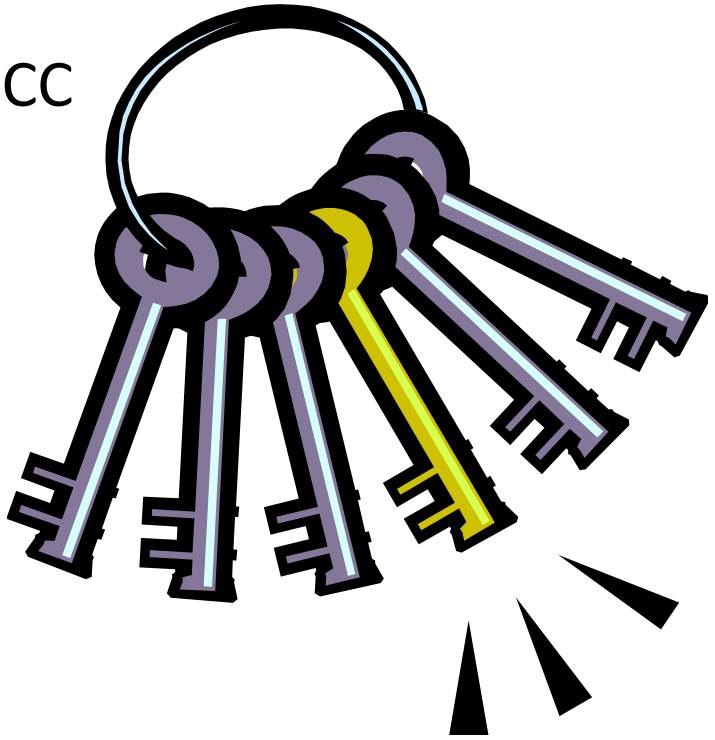
Copyrights and Trademarks

Agenda

- Crypto Levelset
  - Crypto Functionality
  - Clear Key vs Secure Key vs Protected Key
  - Crypto Hardware Technology
- Hardware performance metrics
- Crypto performance data and reports

Crypto Functions

- Data Confidentiality
  - Symmetric – DES/TDES, AES
  - Asymmetric – RSA, Diffie-Hellman, ECC
- Data Integrity
  - Modification Detection
  - Message Authentication
  - Non-repudiation
- Financial Functions
- Key Security & Integrity



Clear Key / Secure Key / Protected Key

- Clear Key – key may be in the clear, at least briefly, somewhere in the environment
- Secure Key – key value does not exist in the clear outside of the HSM (secure, tamper-resistant boundary of the card)
- Protected Key – key value does not exist outside of physical hardware, although the hardware may not be tamper-resistant

z Systems Crypto Hardware

- CP Assist for Crypto Function (CPACF)
  - Clear Key DES/TDES (56-, 112-, 168-bit)
  - Clear Key AES-128, AES-192, AES-256
  - SHA-1, SHA-2, SHA-3, SHAKE
  - Random Numbers
  - Elliptic Curve Public Keys
- Crypto Express
  - Secure Key DES/TDES (56-, 112-, 168-bit)
  - Secure Key AES-128, AES-192, AES-256
  - Financial (PIN) Functions
  - Key Generate/Key Management
  - PKA Public/Private Key
  - Protected Key Support
  - PKCS #11
  - QSA

TechDoc WP100810 – A Synopsis of System z Crypto Hardware

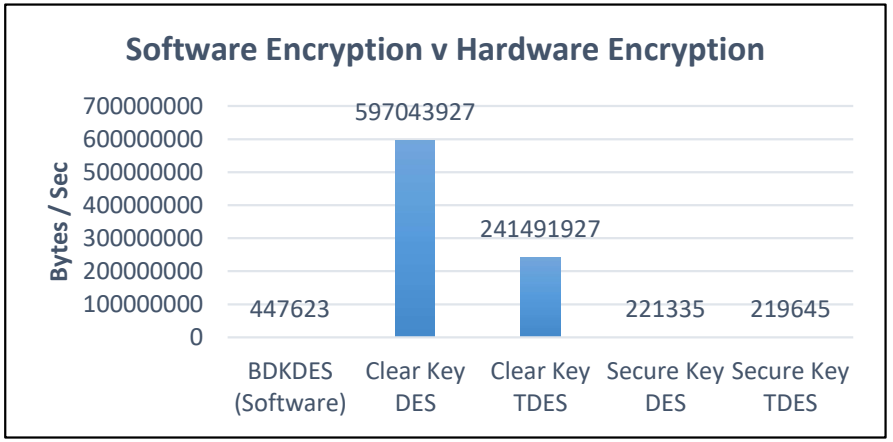
Crypto Card Modes

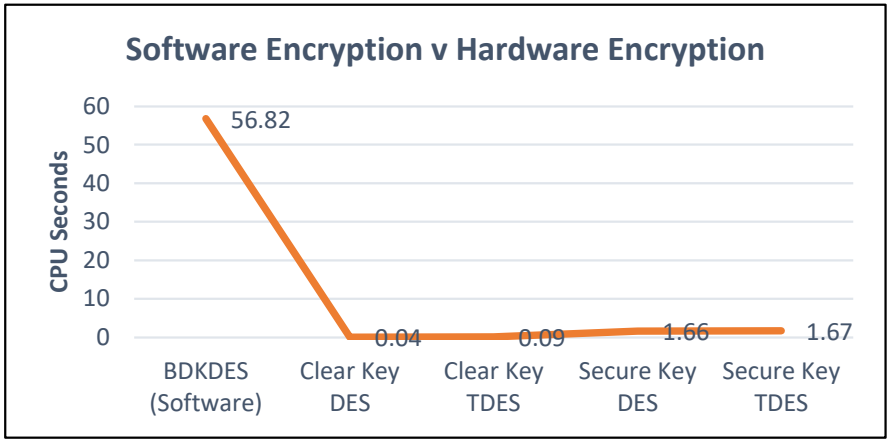
- Coprocessor
  - Secure key support
  - Financial PIN operations
  - Key generation
  - RSA public & private key operations
- Accelerator
  - RSA public key operations only
- EP11 (Enterprise PKCS #11)
  - PKCS #11 clear and secure key operations

Software vs Hardware Encryption

- Adapted from Ernie Nachtigall's TechDoc, WP101240 'IBM z10 DES Cryptographic Performance' https://www.ibm.com/support/pages/ibm-z10-des-cryptographic-hardware-performance-versus-zos-software-des

	Bytes/Sec	CPU Time
BDKDES (Software)	447623	56.82
Clear Key DES	597043927	0.04
Clear Key TDES	241491927	0.09
Secure Key DES	221335	1.66
Secure Key TDES	219645	1.67

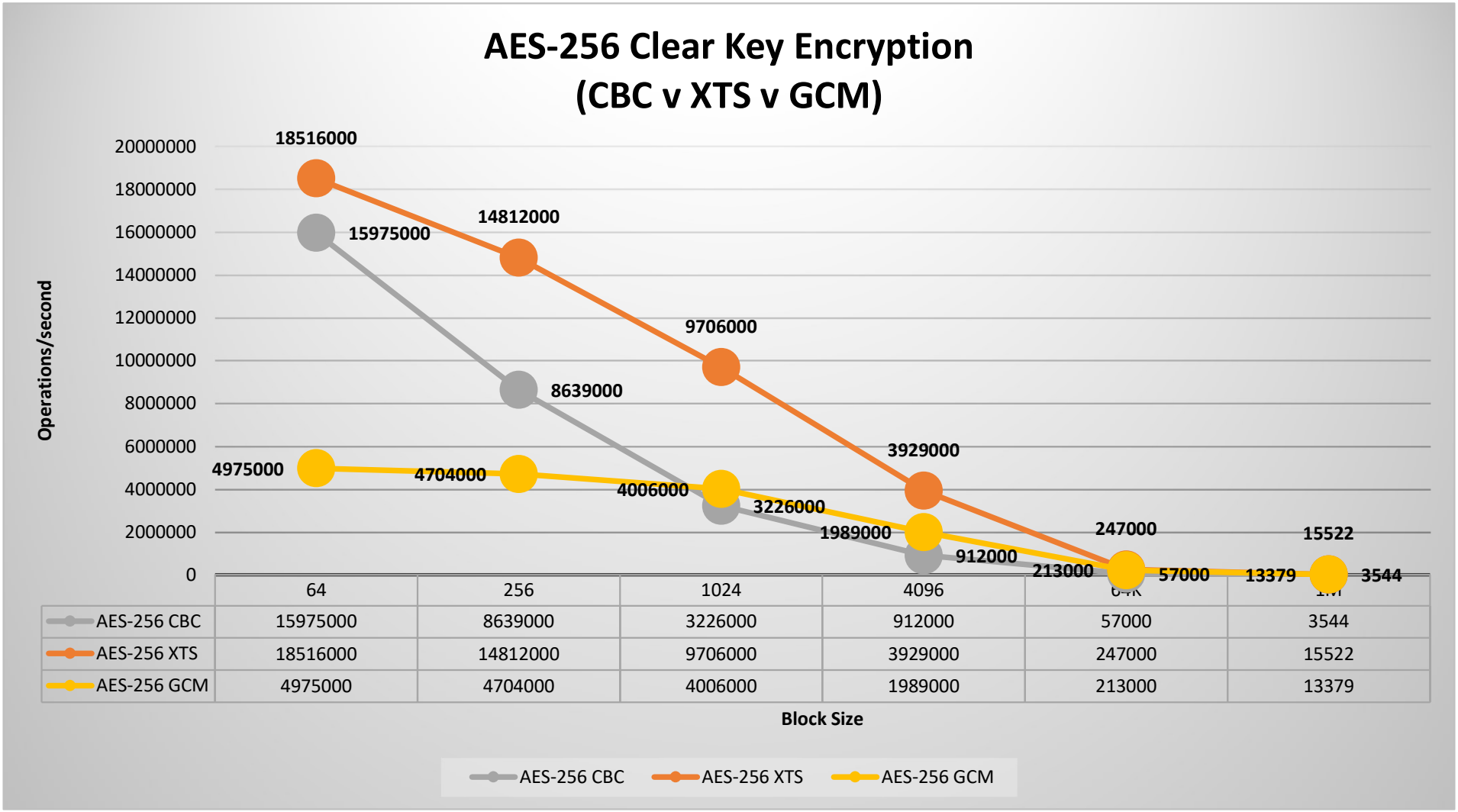




z16 Performance Metrics

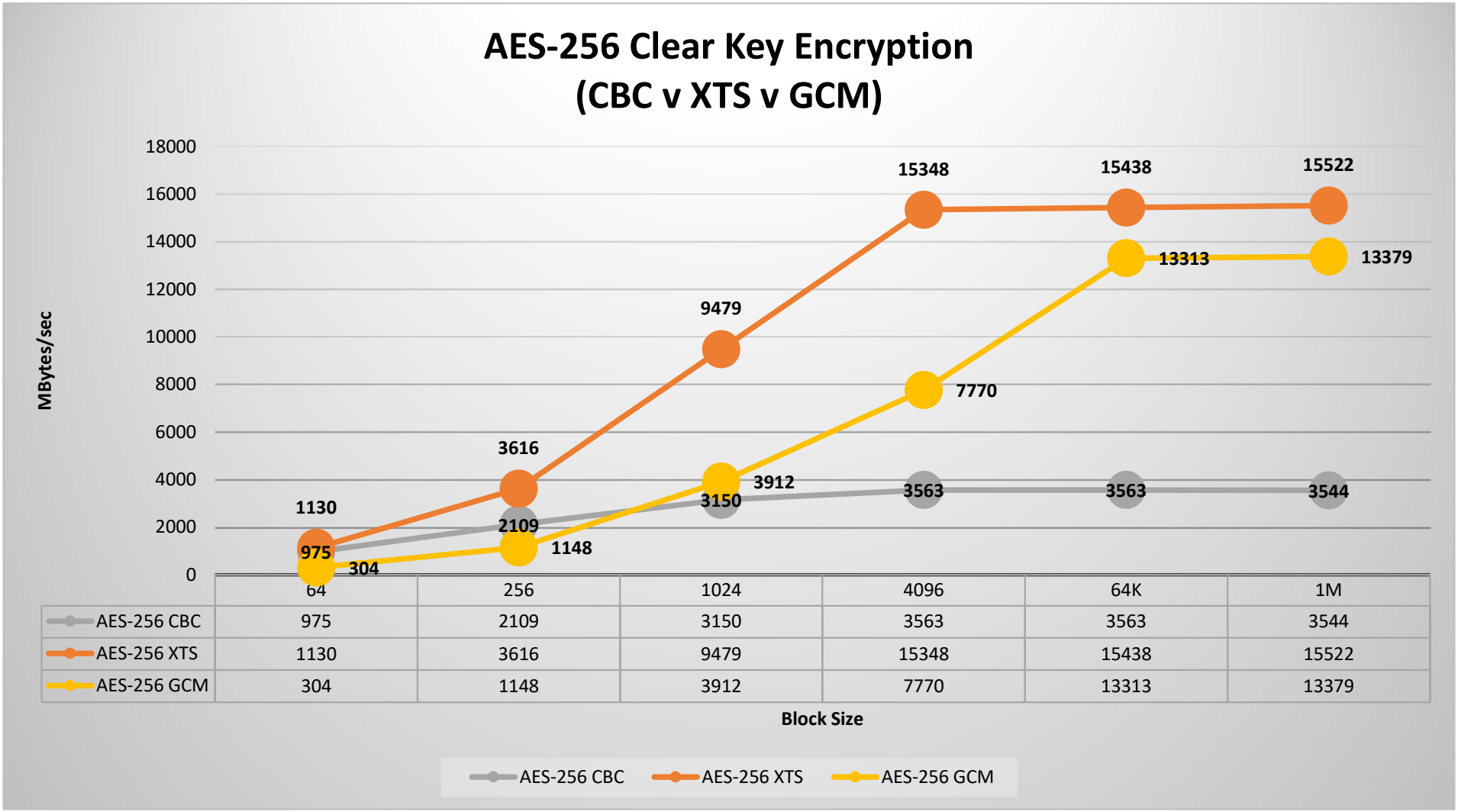
- IBM z16 Performance of Cryptographic Operations (Cryptographic Hardware: CPACF, CEX8S with Quantum-Safe CRYSTALS algorithms) Version 1.0 (March 2023)
  - https://ibm.ent.box.com/s/r6kdgxfyut1gwxlbu3c1zglqhxb50ka8
  - Or maybe Google 'IBM Performance of Cryptographic Operations'
    - Should find z15 and z14, if not z16 White Papers
- Changes (vs previous reports)
  - Charts show operations or Mbytes / second
    - Megabytes = 1,048,576 bytes (previous versions it was 1,000,000 bytes)
  - Added a column to show the delta over the previous generation (the z16 over the z15)

z16 CPACF Clear Key – Operations/second

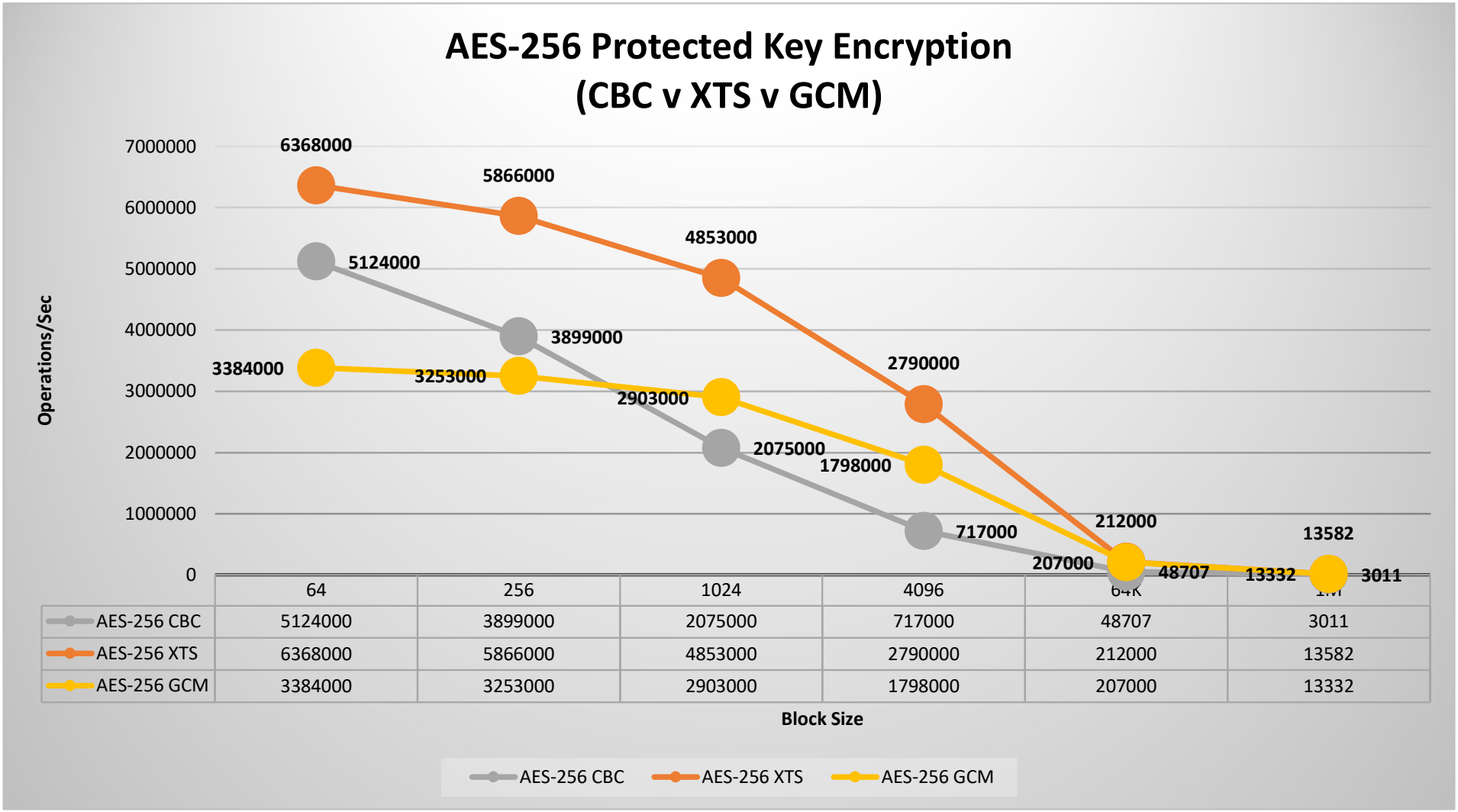


	64	256	1024	4096	64K	1M
AES-256 CBC	15975000	8639000	3226000	912000	57000	3544
AES-256 XTS	18516000	14812000	9706000	3929000	247000	15522
AES-256 GCM	4975000	4704000	4006000	1989000	213000	13379

z16 CPACF Clear Key – Mbytes/second

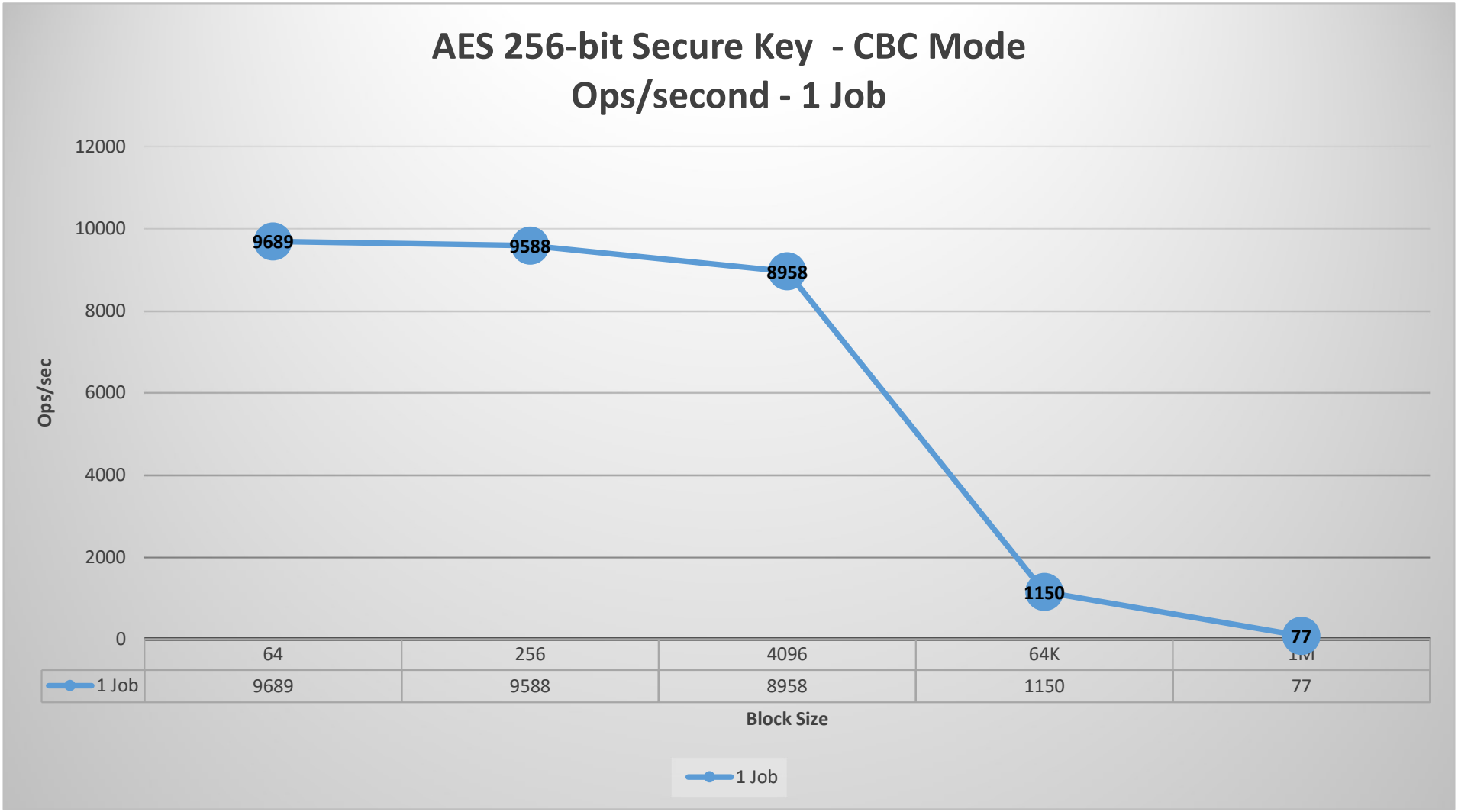


z16 CPACF Protected Key – Operations/second

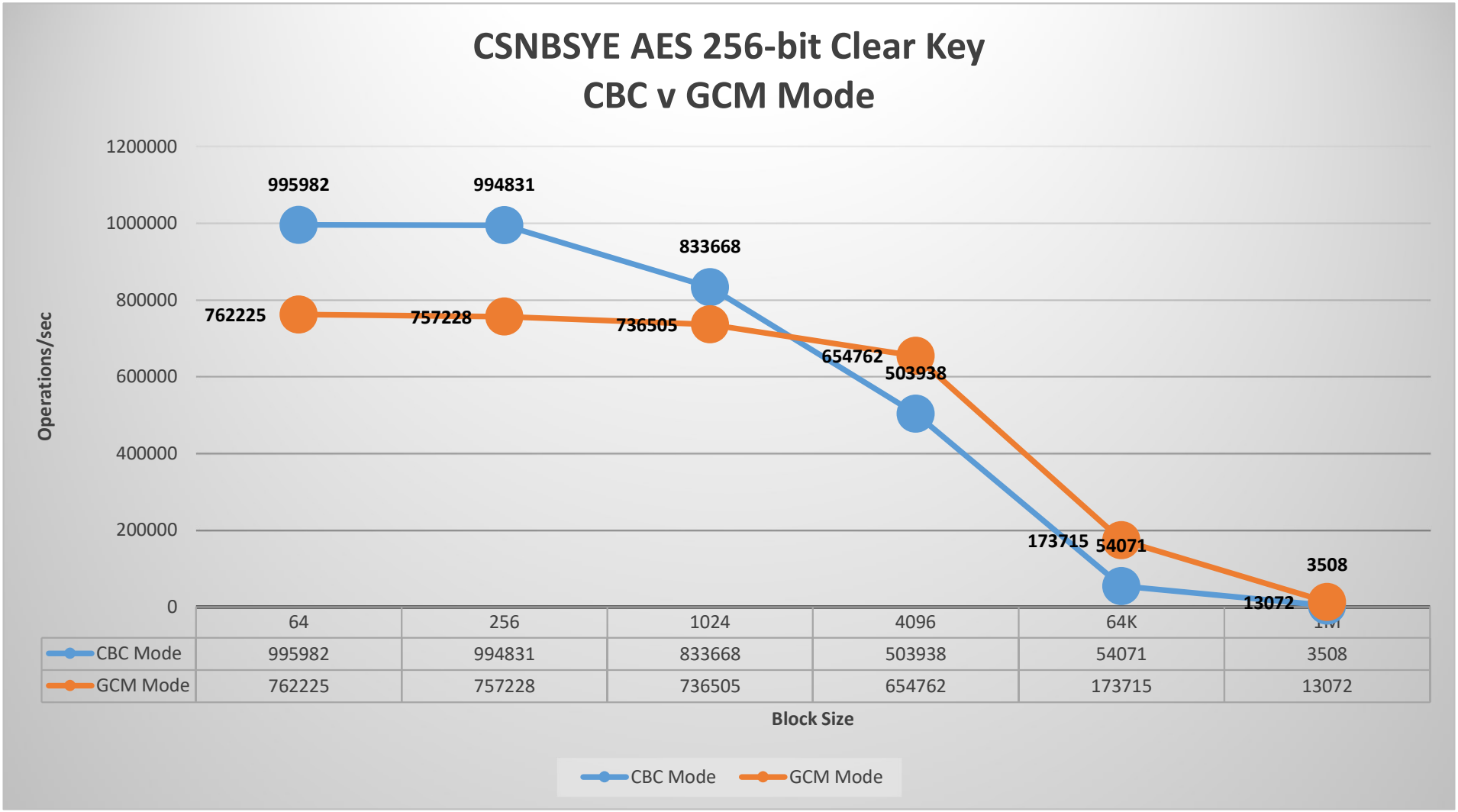


	64	256	1024	4096	64K	1M
AES-256 CBC	5124000	3899000	2075000	717000	48707	3011
AES-256 XTS	6368000	5866000	4853000	2790000	212000	13582
AES-256 GCM	3384000	3253000	2903000	1798000	207000	13332

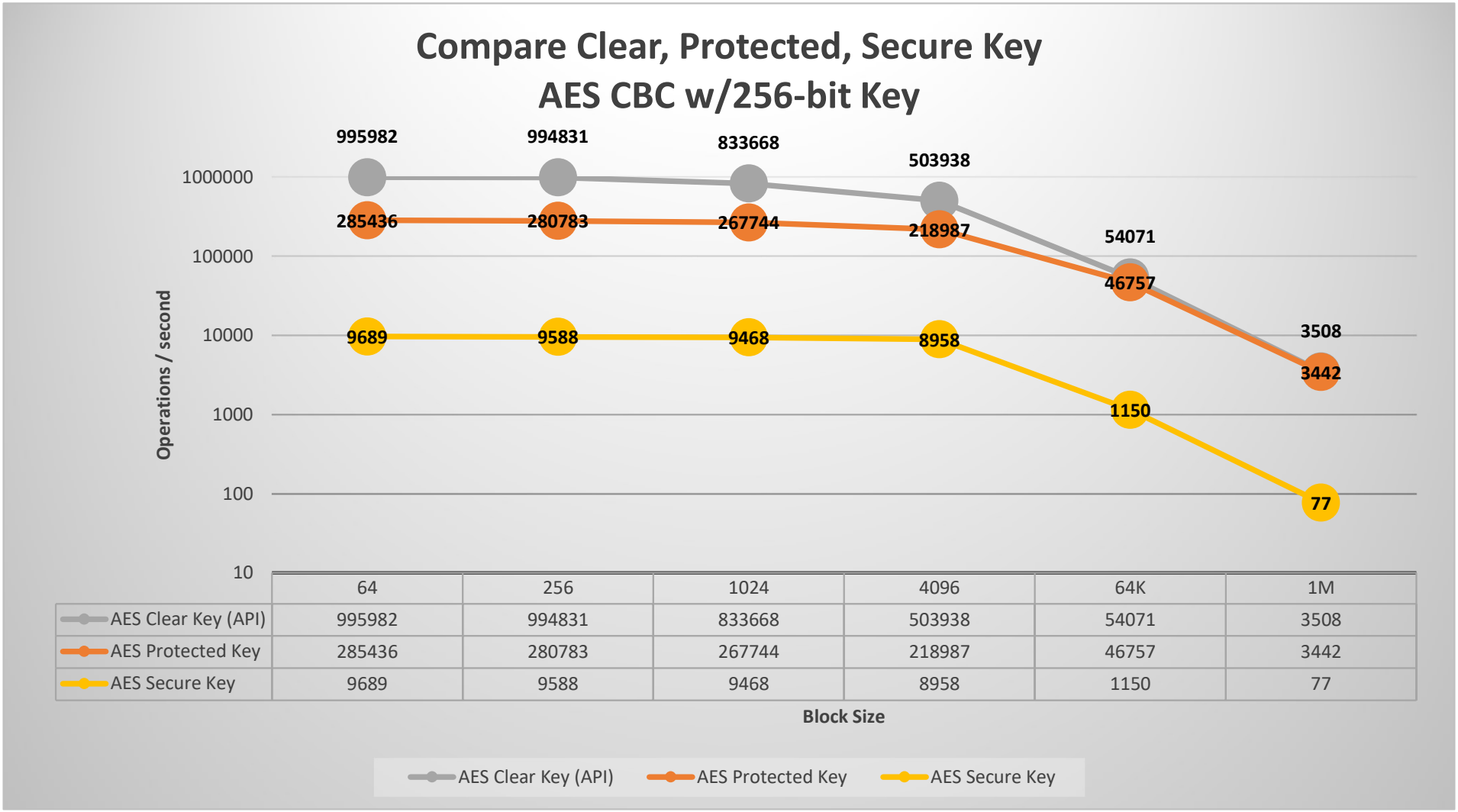
z16 CEX8 Secure Key



z16 ICSF API Clear Key – Operations/second

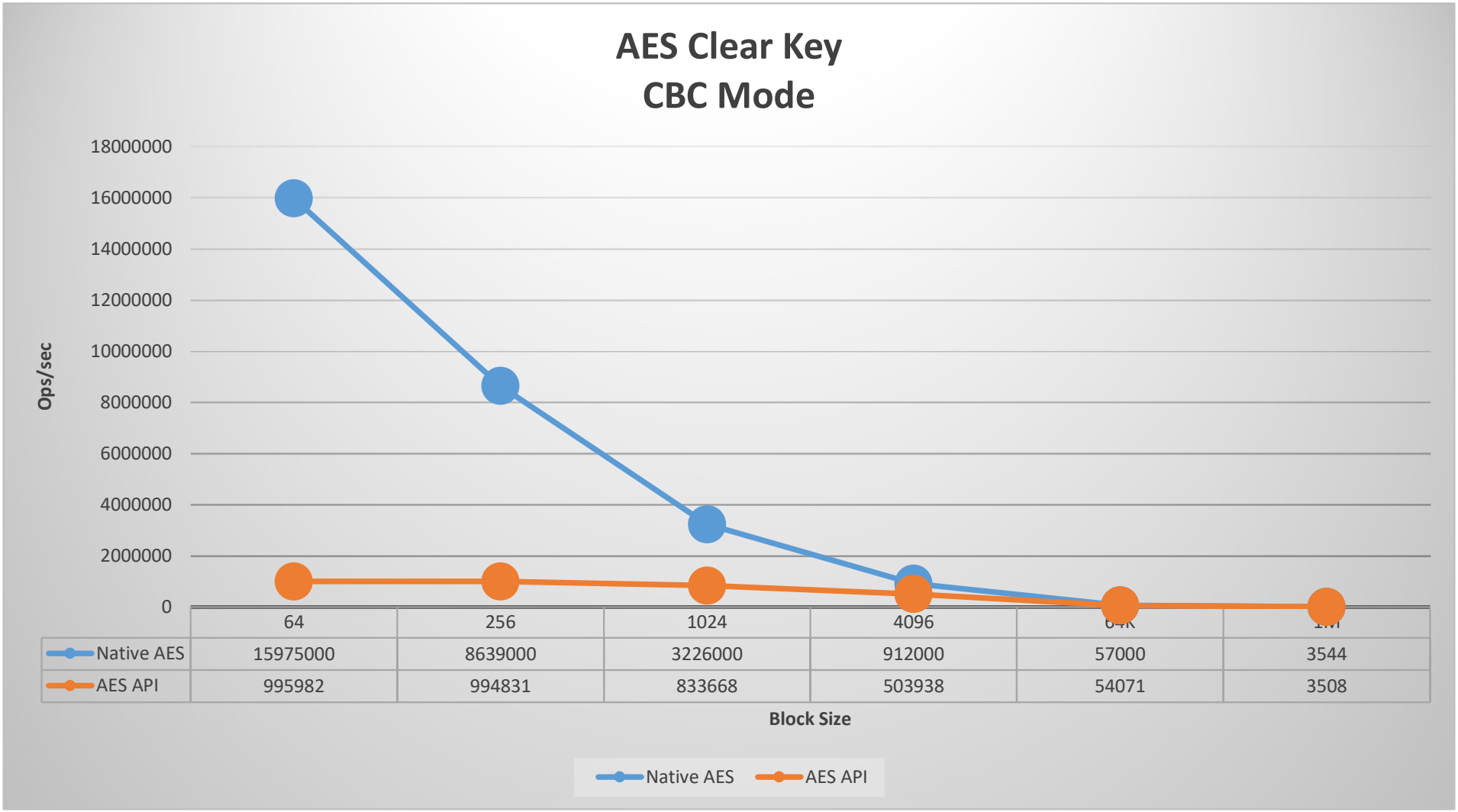


z16 – Clear v Protected v Secure Key (AES 256-bit CBC)



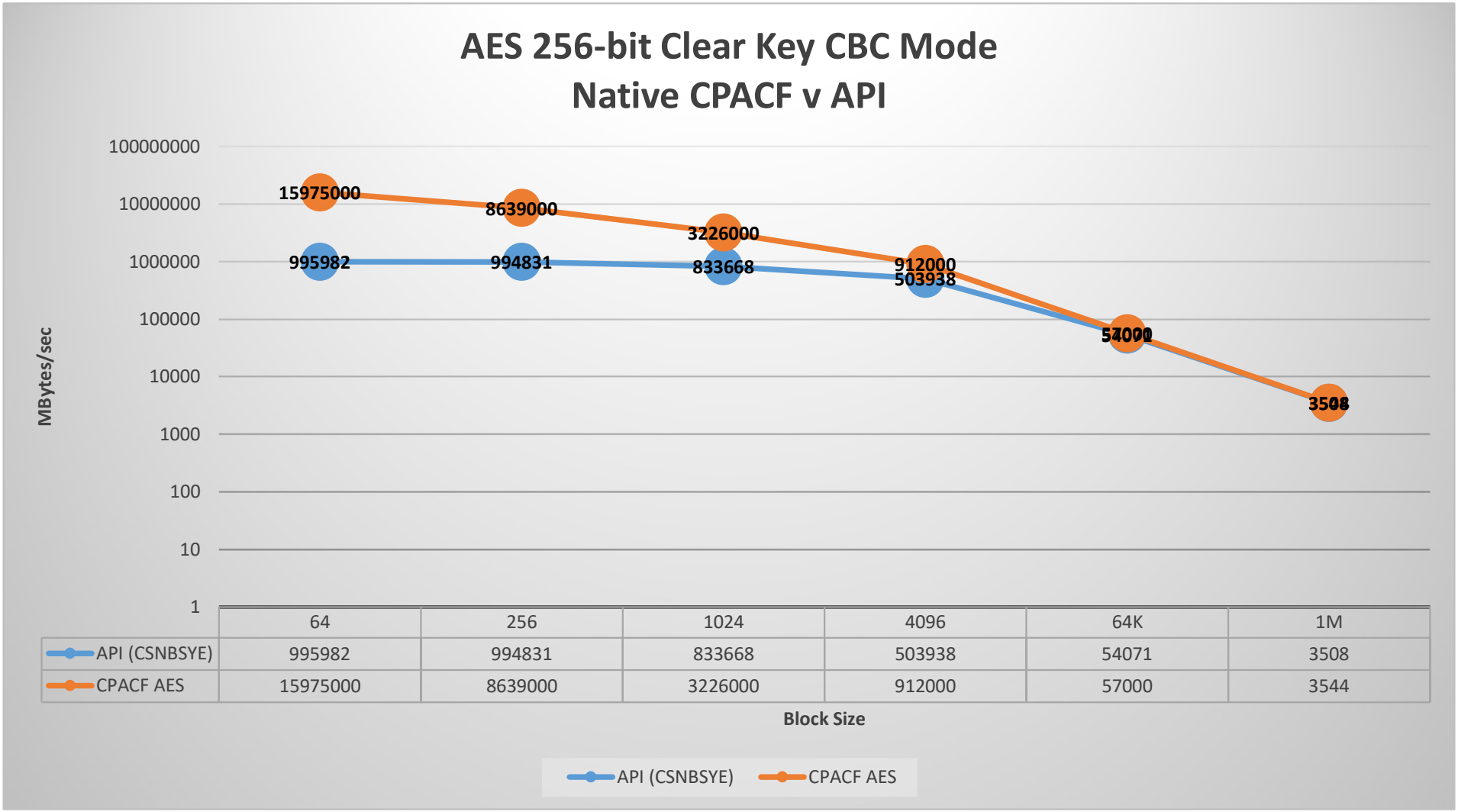
	64	256	1024	4096	64K	1M
AES Clear Key (API)	995982	994831	833668	503938	54071	3508
AES Protected Key	285436	280783	267744	218987	46757	3442
AES Secure Key	9689	9588	9468	8958	1150	77

Compare Native Instructions to APIs (Ops)



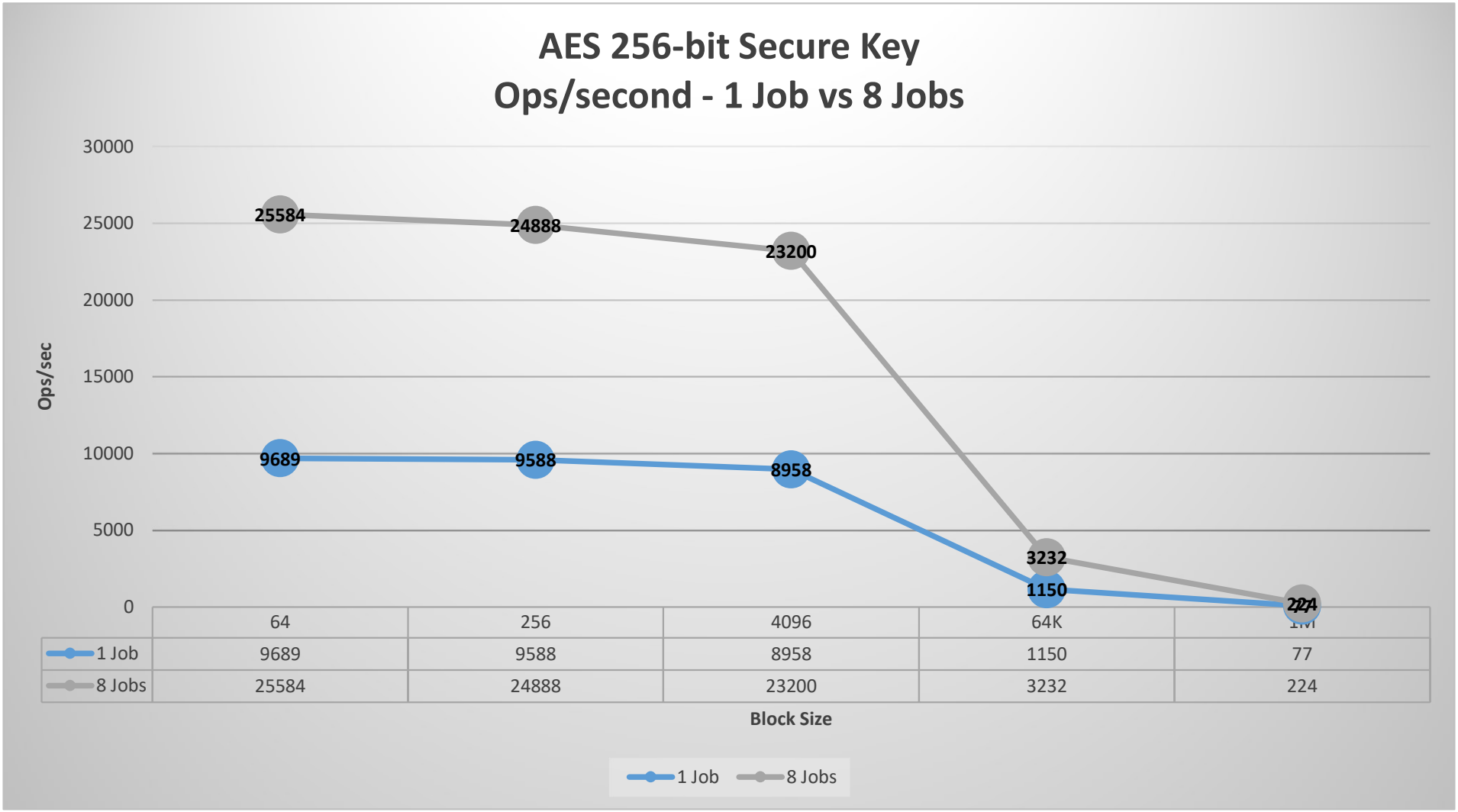
	64	256	1024	4096	64K	1M
Native AES	15975000	8639000	3226000	912000	57000	3544
AES API	995982	994831	833668	503938	54071	3508

Compare Native Instructions to APIs (Mbytes)



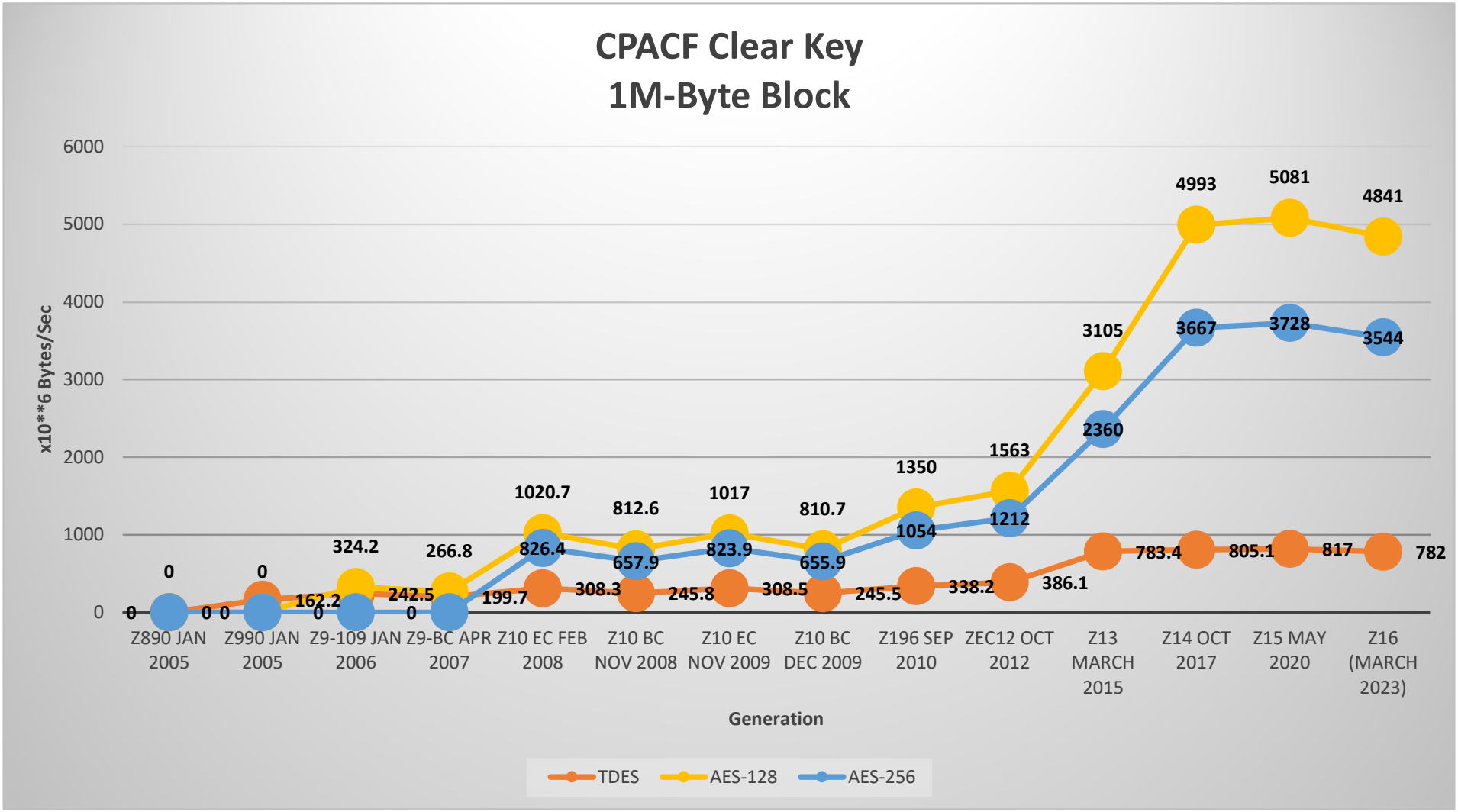
	64	256	1024	4096	64K	1M
API (CSNBSYE)	995982	994831	833668	503938	54071	3508
CPACF AES	15975000	8639000	3226000	912000	57000	3544

Secure Key – Multiple Threads

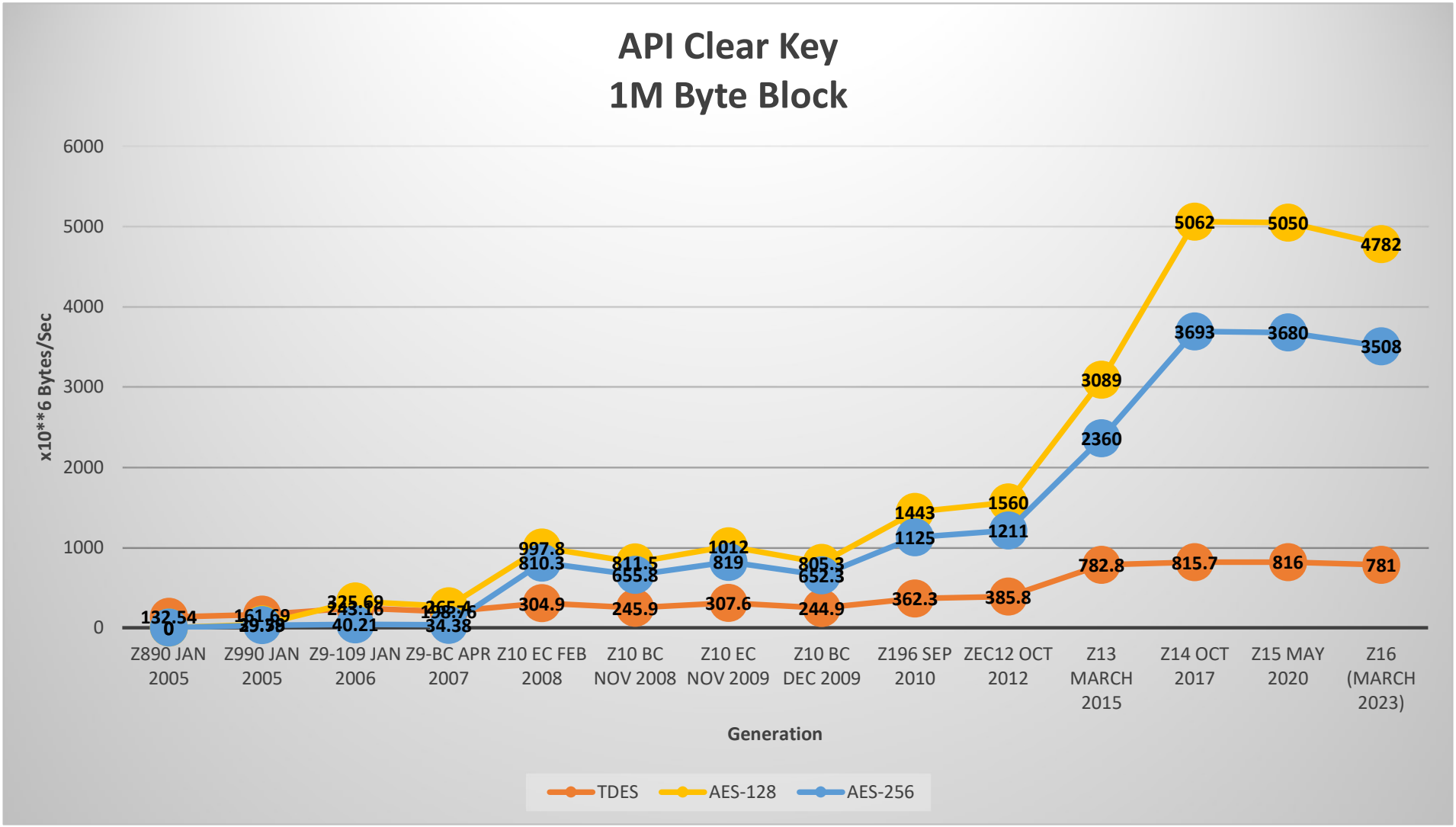


	64	256	4096	64K	1M
1 Job	9689	9588	8958	1150	77
8 Jobs	25584	24888	23200	3232	224

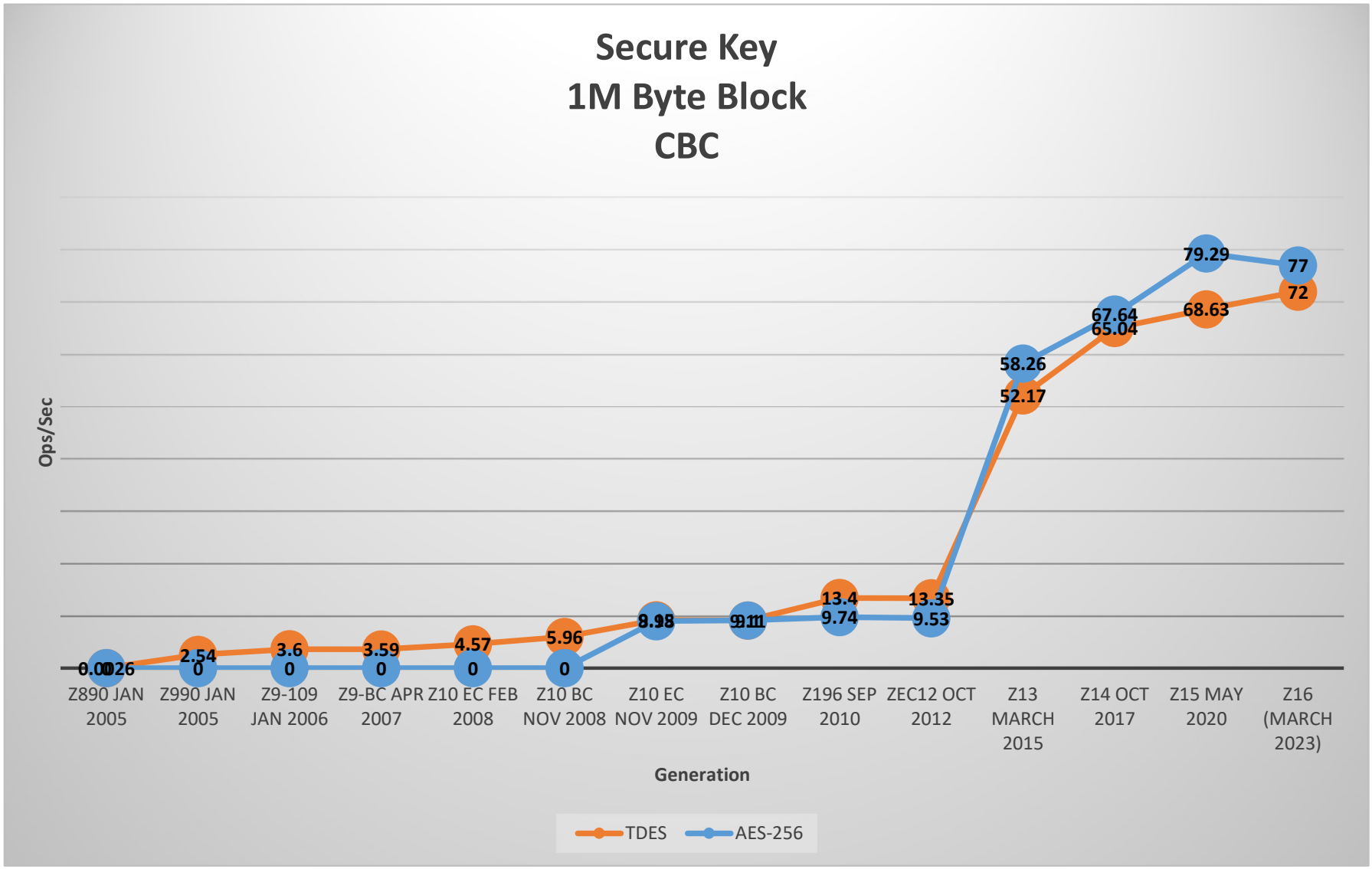
Crypto performance across CECs - CPACF



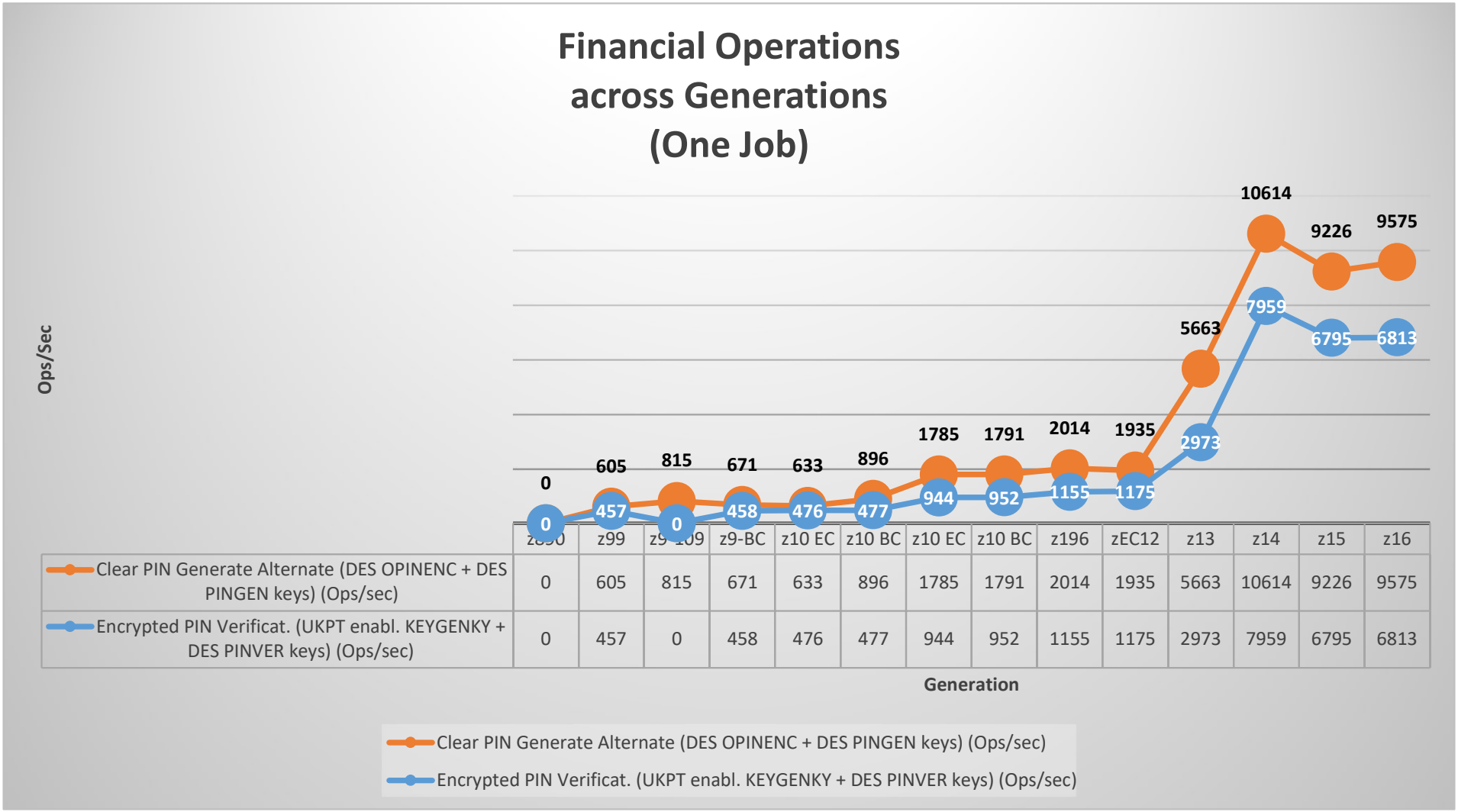
Crypto performance across CECs - CPACF



Crypto performance across CECs - CPACF

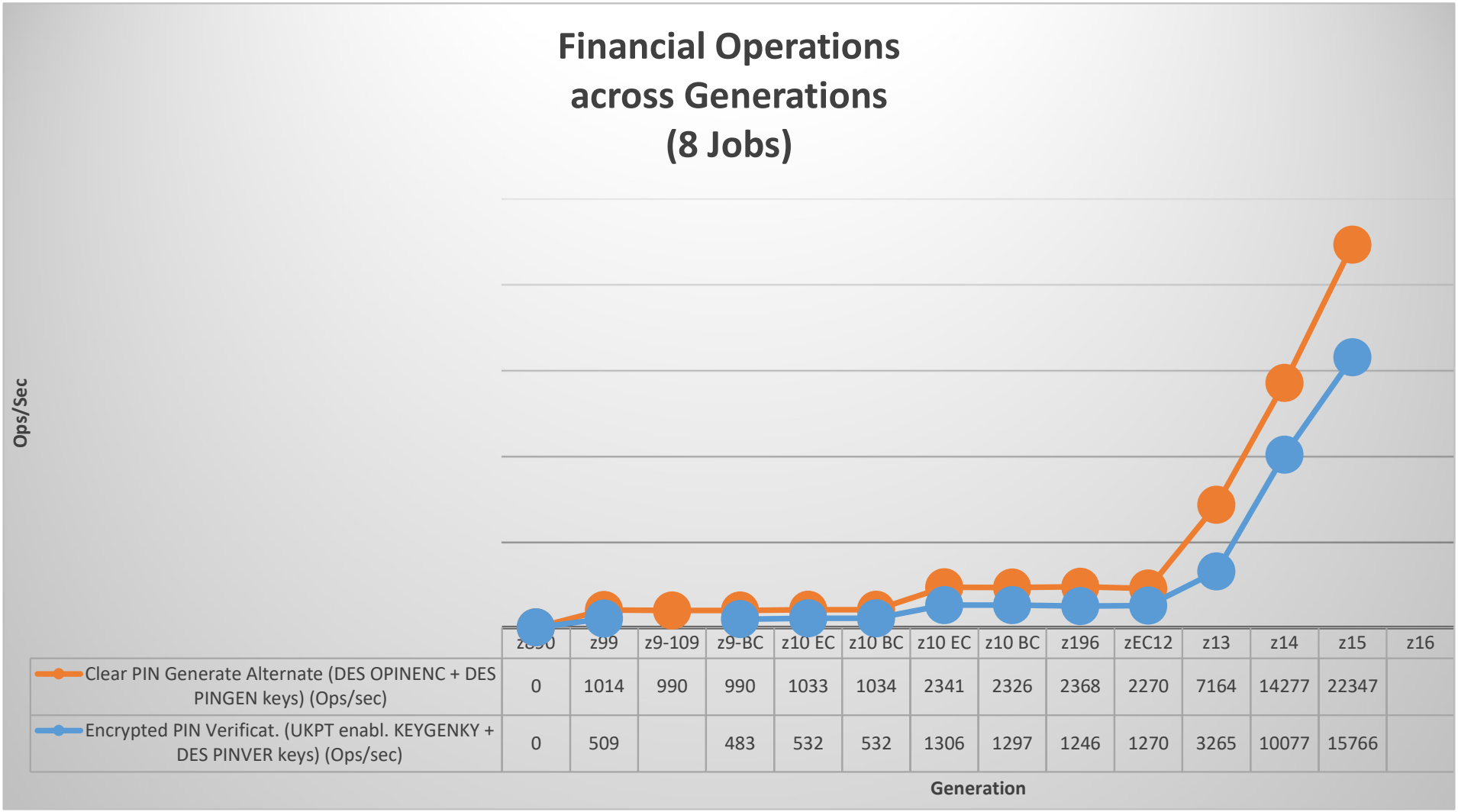


Crypto Performance across CECs – selected APIs (One Job)



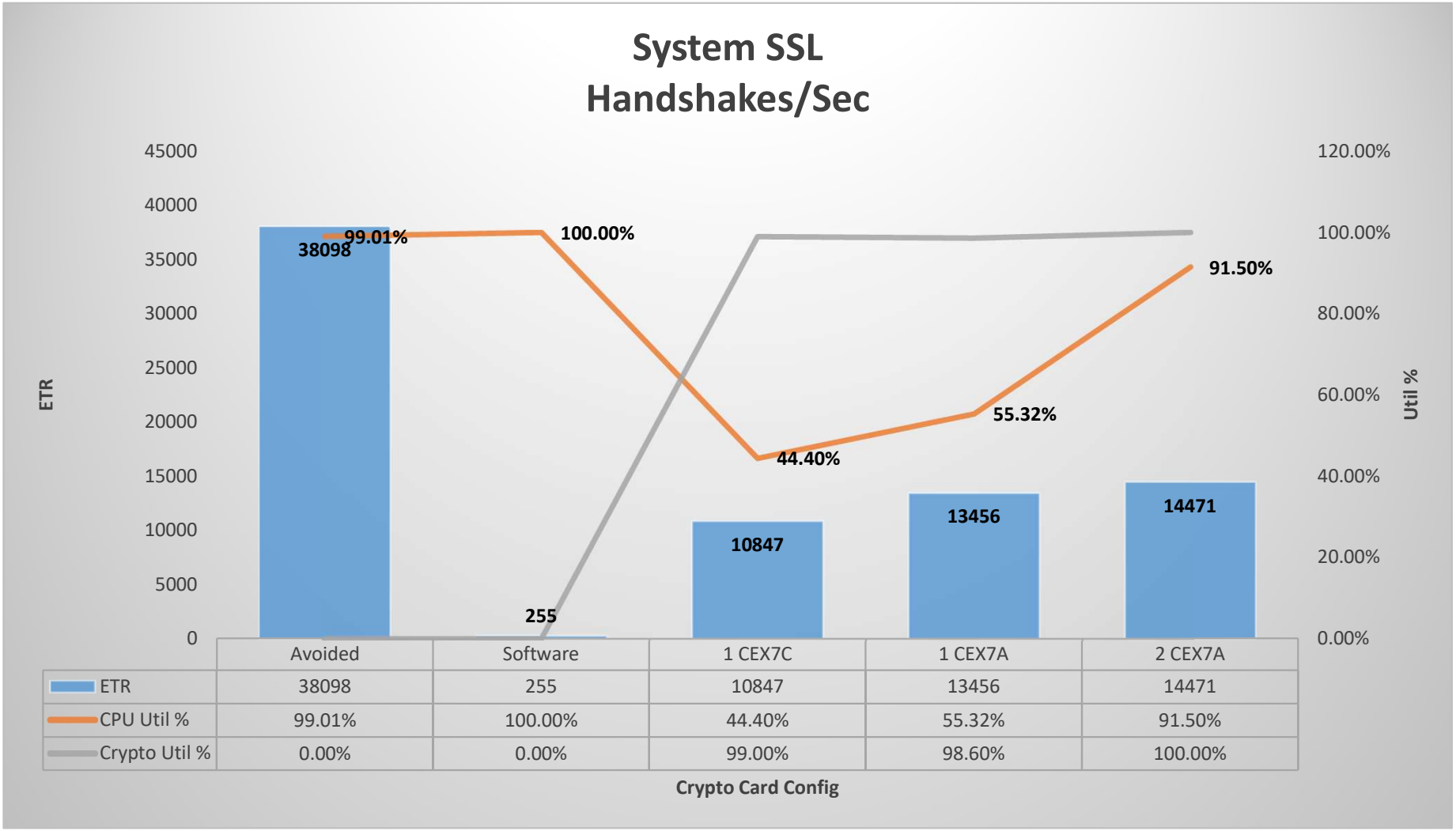
	z890	z99	z9-109	z9-BC	z10 EC	z10 BC	z10 EC	z10 BC	z196	zEC12	z13	z14	z15	z16
Clear PIN Generate Alternate (DES OPINENC + DES PINGEN keys) (Ops/sec)	0	605	815	671	633	896	1785	1791	2014	1935	5663	10614	9226	9575
Encrypted PIN Verificat. (UKPT enabl. KEYGENKY + DES PINVER keys) (Ops/sec)	0	457	0	458	476	477	944	952	1155	1175	2973	7959	6795	6813

Crypto Performance across CECs – selected APIs (8 Jobs)



	z890	z99	z9-109	z9-BC	z10 EC	z10 BC	z10 EC	z10 BC	z196	zEC12	z13	z14	z15	z16
Clear PIN Generate Alternate (DES OPINENC + DES PINGEN keys) (Ops/sec)	0	1014	990	990	1033	1034	2341	2326	2368	2270	7164	14277	22347	
Encrypted PIN Verificat. (UKPT enabl. KEYGENKY + DES PINVER keys) (Ops/sec)	0	509		483	532	532	1306	1297	1246	1270	3265	10077	15766	

System SSL Performance – z15

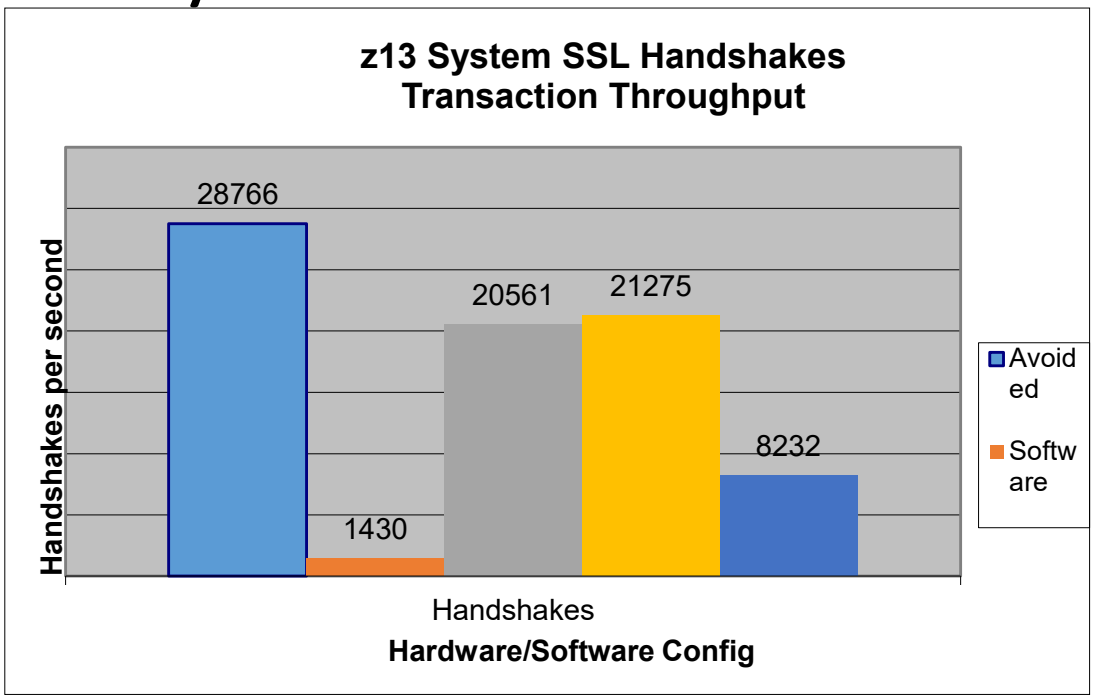


	Avoided	Software	1 CEX7C	1 CEX7A	2 CEX7A
ETR	38098	255	10847	13456	14471
CPU Util %	99.01%	100.00%	44.40%	55.32%	91.50%
Crypto Util %	0.00%	0.00%	99.00%	98.60%	100.00%

IBM z15 Model 8561-770 (4 CPs)

z/OS Version 2 Release 4 (z/OS V2.4) and ICSF FMID HCR77D1

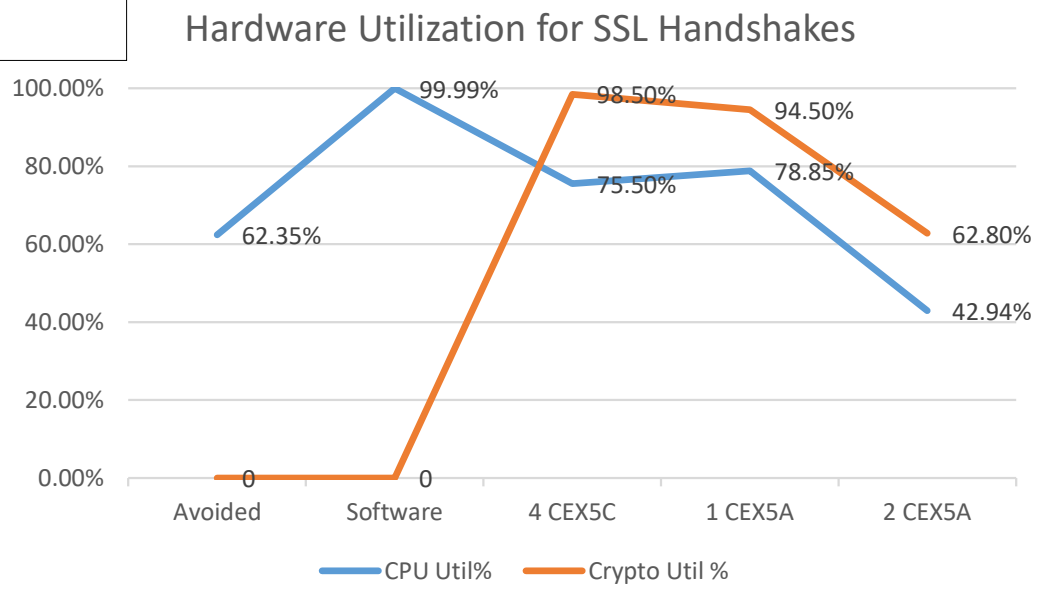
System SSL Performance – z13



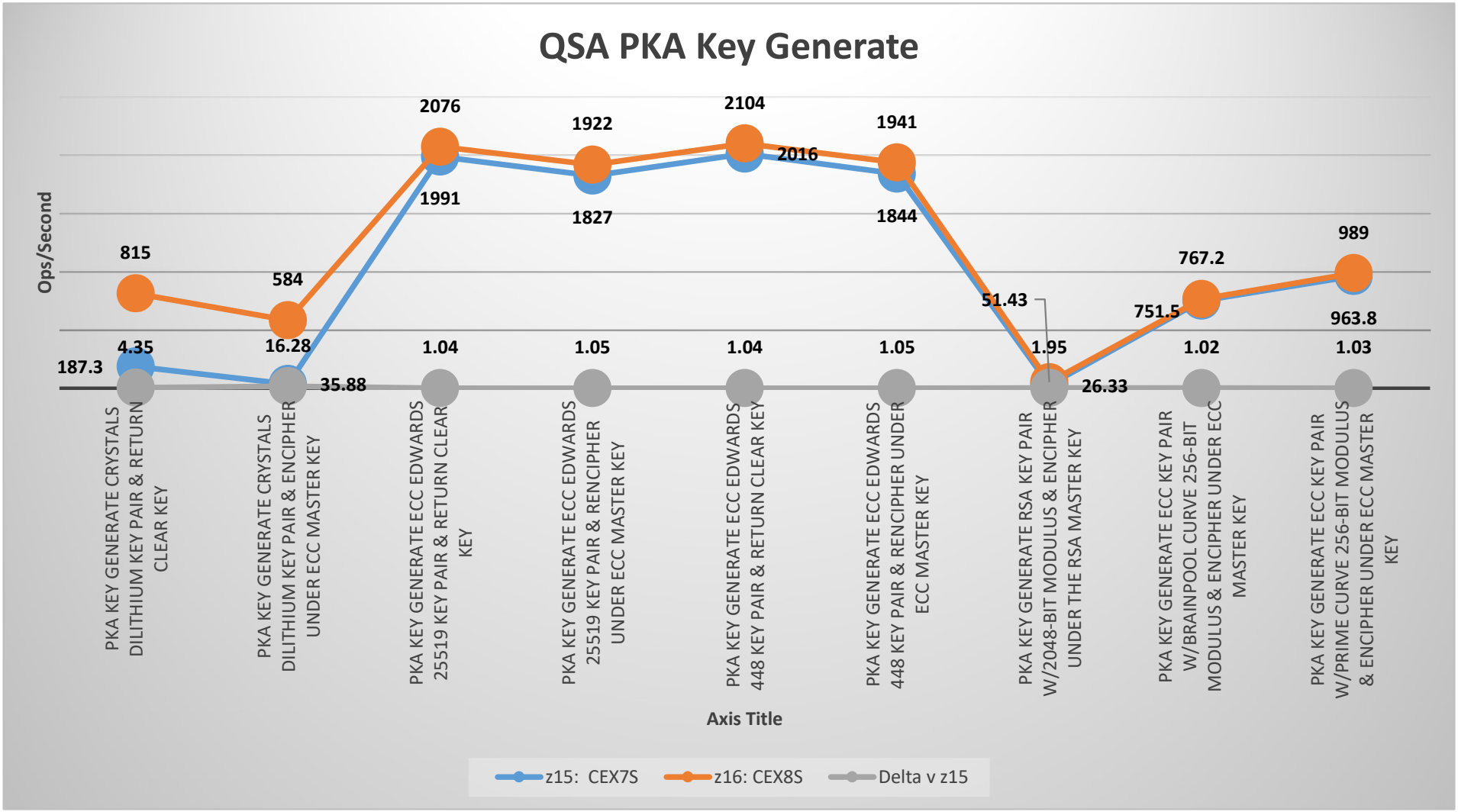
Caching SID/Client Authenti-cation	Hand-shakes	ETR	CPU Util%	Crypto Util %
100%/No	Avoided	28766	62.35%	NA
No/No	Software	1430	99.99%	NA
No/No	4 CEX5C	20561	75.50%	98.50%
No/No	1 CEX5A	21275	78.85%	94.50%
No/Yes	2 CEX5A	8232	42.94%	62.80%

IBM z13 Model 2964-N96 (4 CPs)

z/OS Version 2 Release 1 (z/OS V2.1)
and ICSF FMID HCR77B0



QSA Enhancements



CPU Measurement Facility

Cntr #	Counter	Cntr #	Counter	Cntr #	Counter
64	PRNG function count	72	DEA function count	80	ECC function count
65	PRNG cycle count	73	DEA cycle count	81	ECC cycle count
66	PRNG blocked function count	74	DEA blocked function count	82	ECC blocked function count
67	PRNG blocked cycle count	75	DEA blocked cycle count	83	ECC blocked cycle count
68	SHA function count	76	AES function count		
69	SHA cycle count	77	AES cycle count		
70	SHA blocked function count	76	AES blocked function count		
71	SHA blocked cycle count	77	AES blockedcycle count		

- Provides hardware instrumentation data for production systems
- CPU MF Counters also useful for performance analysis
- Data gathering controlled through z/OS HIS (HW Instrumentation Services)
- Supplements current performance data from SMF, RMF, DB2, CICS, etc.
- Measure (count) CPACF Usage
- Recorded in SMF Type 113

RMF Crypto Hardware Activity Report

(From z/OS RMF Report Analysis 2.5, SC34-2665-50)

C R Y P T O H A R D W A R E A C T I V I T Y

PAGE 1

z/OS V2R5 SYSTEM ID TRX2 DATE 09/30/2021 INTERVAL 14.59.998
RPT VERSION V2R5 RMF TIME 11.00.00 CYCLE 1.000 SECONDS

-------- CRYPTOGRAPHIC CCA COPROCESSOR ----------

		---------- LPAR ----------			---------- CPC ----------			----- LPAR -----	------- CPC ------
TYPE	ID	RATE	EXEC TIME	UTIL%	RATE	EXEC TIME	UTIL%	KEY-GEN RATE	KEY-GEN RATE
CEX5C	0	0.00	0.000	0.0	0.00	0.000	0.0	0.00	0.00
	1	1997	0.209	41.7	4873	0.205	99.8	0.86	0.86
CEX6C	5	4290	0.092	39.4	9009	0.111	99.6	3.52	3.52
	6	4349	0.091	39.4	9138	0.109	99.5	3.83	3.83
	7	4352	0.090	39.3	9144	0.109	99.5	3.61	3.61
	8	4362	0.090	39.4	9165	0.109	99.5	4.05	4.05
	9	0.00	0.000	0.0	0.00	0.000	0.0	0.00	0.00
	10	0.00	0.000	0.0	0.00	0.000	0.0	0.00	0.00
	11	0.00	0.000	0.0	0.00	0.000	0.0	0.00	0.00
	12	0.00	0.000	0.0	0.00	0.000	0.0	0.00	0.00

SMF Type 70 Subtype 2 – RMF Processor Activity

RMF Crypto Hardware Activity Report (Cont.)

-------- CRYPTOGRAPHIC PKCS11 COPROCESSOR ----------

		---------- LPAR ----------			---------- CPC ----------				---------- LPAR ----------			---------- CPC ----------		
TYPE	ID	RATE	EXEC TIME	UTIL%	RATE	EXEC TIME	UTIL%	FUNCTION	RATE	EXEC TIME	UTIL%	RATE	EXEC TIME	UTIL%
CEX5P	3	461.8	1.004	46.4	1005	0.995	99.9	ASYM FAST	253.8	0.947	24.0	470.4	1.009	47.5
								ASYM GEN	0.00	0.000	0.0	0.38	2.067	0.1
								ASYM SLOW	186.5	1.081	20.2	491.6	1.011	49.7
								SYMM COMPLETE	21.48	1.012	2.2	42.52	0.638	2.7
								SYMM PARTIAL	0.00	0.000	0.0	0.00	0.000	0.0

SMF Type 70 Subtype 2 – RMF Processor Activity

RMF Crypto Hardware Activity Report (Cont.)

-------- CRYPTOGRAPHIC ACCELERATOR ----------

		-------- LPAR ---------		--------- CPC ---------			--------- LPAR --------		--------- CPC ---------	
TYPE	ID	RATE	EXEC TIME	UTIL%	RATE	EXEC TIME	UTIL%	FUNCTION	RATE	EXEC TIME	UTIL%	RATE	EXEC TIME	UTIL%
CEX5A	2				15043	0.066	99.7	RSA ME 1024				1538	0.031	4.8
								RSA ME 2048				5965	0.026	15.6
								RSA ME 4096				2524	0.064	16.3
								RSA CRT 1024				4382	0.042	18.2
								RSA CRT 2048				246.2	0.207	5.1
								RSA CRT 4096				387.8	1.025	39.7

SMF Type 70 Subtype 2 – RMF Processor Activity

RMF Crypto Hardware Activity Report (Cont.)

-------- ICSF SERVICES ----------

---- ENCRYPTION ----- ---- DECRYPTION ----- -------- HASH --------- ------ PIN -------

	SDES	TDES	AES	SDES	TDES	AES	SHA-1	SHA-256	SHA-512	TRANSLATE	VERIFY
RATE	2399	1557	0.00	0.00	0.00	0.00	192K	0.00	0.00	0.00	0.00
SIZE	2622	5057	0.00	0.00	0.00	0.00	9393	0.00	0.00		

-------- MAC -------- ------ AES MAC ---- ----- RSA DSIG ----- ----- ECC DSIG ---- - FORMAT PRESERVING ENCRYPTION –

	GENERATE	VERIFY	GENERATE	VERIFY	GENERATE	VERIFY	GENERATE	VERIFY	ENCIPHER	DECIPHER	TRANSLATE
RATE	158.6	0.00	0.00	0.00	2753	1734	0.00	0.00	0.00	0.00	0.00
SIZE	9545	0.00	0.00	0.00					0.00	0.00	0.00

----- QSA DSIG ---- -- FEISTEL-BASED ENCRYPTION –

	GENERATE	VERIFY	ENCIPHER	DECIPHER	TRANSLATE
RATE	158.6	0.00	0.00	0.00	0.00
SIZE			0.00	0.00	0.00

SMF Type 70 Subtype 2 – RMF Processor Activity

RMF Monitor III (z/OS 2.4)

- SYSPLEX
  - CRYOVW – Crypto hardware overview (CRO)
  - CRYACC – Crypto accelerator activity (CRA)
  - CRYPKC – Crypto PKCS11 coprocessor activity (CRP)

RMF Overview Report – Type 70-1

OVW(ENCRMSU(LACSCR))

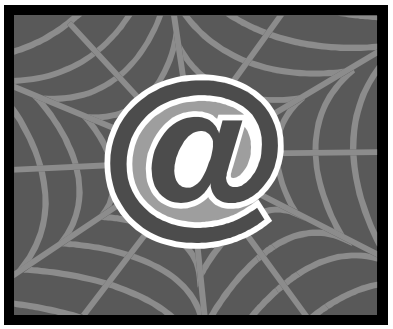
```
          R M F     O V E R V I E W
  z/OS V2R2        SYSTEM ID JA0                        START 0
      CONVERTED TO z/OS V2R3 RMF                 END 0
NUMBER OF INTERVALS 14       TOTAL LENGTH OF INTERVALS 07.00.00
    DATE     TIME         INT              ENCRMSU
    MM/DD    HH.MM.SS     HH.MM.SS
    07/31    14.00.00     00.30.00               0
    07/31    14.30.00     00.30.00               0
    07/31    15.00.00     00.30.00               0
    07/31    15.30.00     00.30.00               1
    07/31    16.00.00     00.30.00               1
    07/31    16.30.00     00.30.00               1
    07/31    17.00.00     00.30.00               1
    07/31    17.30.00     00.30.00               1
    07/31    18.00.00     00.30.00               2
    07/31    18.30.00     00.30.00               2
    07/31    19.00.00     00.30.00               2
    07/31    19.30.00     00.30.00               2
    07/31    20.00.00     00.30.00               2
    07/31    20.30.00     00.30.00               2
```

SMF70LACCR Long-term average of CPU service (millions of service units) consumed by DFSMS data set encryption (z14 & later)

Summary

- There is performance data available, but …
- Your implementation will be the most significant factor in terms of performance
- Consider your ICSF options (and their impact on performance)
- Start collecting performance data now, and look for trends
- The performance reporting has gotten better, hopefully it will get even better

IBM Manuals & Redbooks



- SC14-7507 ICSF System Programmer's Guide
- SC34-2665 z/OS RMF Report Analysis 2.1
- SA22-7630 z/OS System Measurement Facilities (SMF)
- SG24-6645 Effective zSeries Performance Monitoring Using Resource Measurement Facility
- REDP-4358 Monitoring System z Cryptographic Services

Crypto Performance Whitepapers

- z16
  - https://ibm.ent.box.com/s/r6kdgxfyut1gwxlbu3c1zglqhxb50ka8
- z15
  - https://www.ibm.com/downloads/cas/6K2653EJ
- z14
  - https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSL03607USEN
- z13
  - https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSW03283USEN
- z/OS Communications Server Performance Index
  - http://www.ibm.com/support/docview.wss?uid=swg27005

Questions …