MAINFRAME CRYPTO

Unscrambling the Complexity of Crypto!

Crypto Performance z15 Update

Greg Boyd

gregboyd@mainframecrypto.com

THE Z EXCHANGE

November 2020

Copyrights and Trademarks

- Copyright © 2020 Greg Boyd, Mainframe Crypto, LLC. All rights reserved.
- Presentation based on material copyrighted by IBM, and developed by myself, as well as many others that I worked with over the past 30+ years

- All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. IBM, System z, zEnterprise and z/OS are trademarks of International Business Machines Corporation in the United States, other countries, or both. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.
- **THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY**. Greg Boyd and Mainframe Crypto, LLC assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will Greg Boyd or Mainframe Crypto, LLC be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if expressly advised in advance of the possibility of such damages.

Agenda

- Crypto Levelset
  - Crypto Functionality
  - Clear Key vs Secure Key vs Protected Key
  - Crypto Hardware Technology
- Hardware performance metrics
- Operational factors
- 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)
  - DES/TDES (56-, 112-, 168-bit)
  - AES-128, AES-192, AES-256
  - SHA-1, SHA-2, SHA-3, SHAKE
  - Random Numbers
  - Elliptic Curve
- Crypto Express
  - Secure Key DES/TDES
  - Secure Key AES
  - Financial (PIN) Functions
  - Key Generate/Key Management
  - PKA Public/Private Key
  - Protected Key Support
  - PKCS #11

TechDoc WP100810 – A Synopsis of System z Crypto Hardware

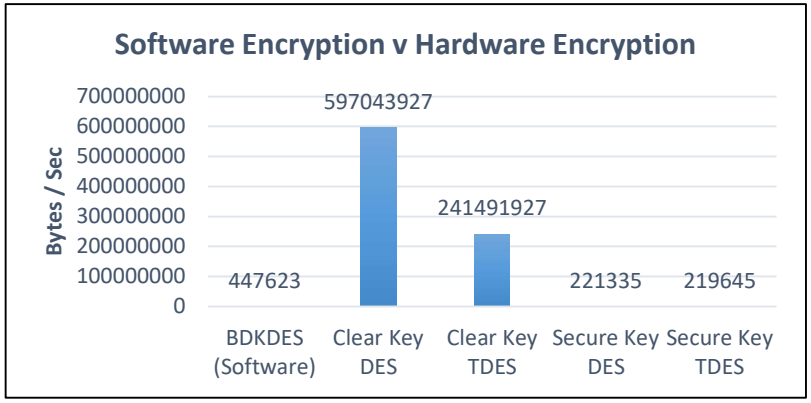
Crypto Card Modes

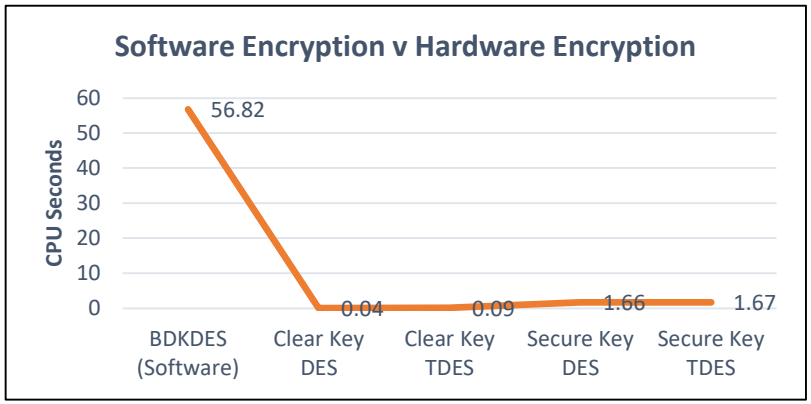
- Coprocessor
  - Secure key support
  - Financial PIN operations
  - Key generation
  - RSA public & private key operations
- Accelerator
  - RSA public key operations only
- EP11 (Enterprise PKCS #11)
  - PKCS #11 clear and secure key operations

Software vs Hardware Encryption

- Adapted from Ernie Nachtigall's TechDoc, WP101240 'IBM z10 DES Cryptographic Performance' available at http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101240

	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

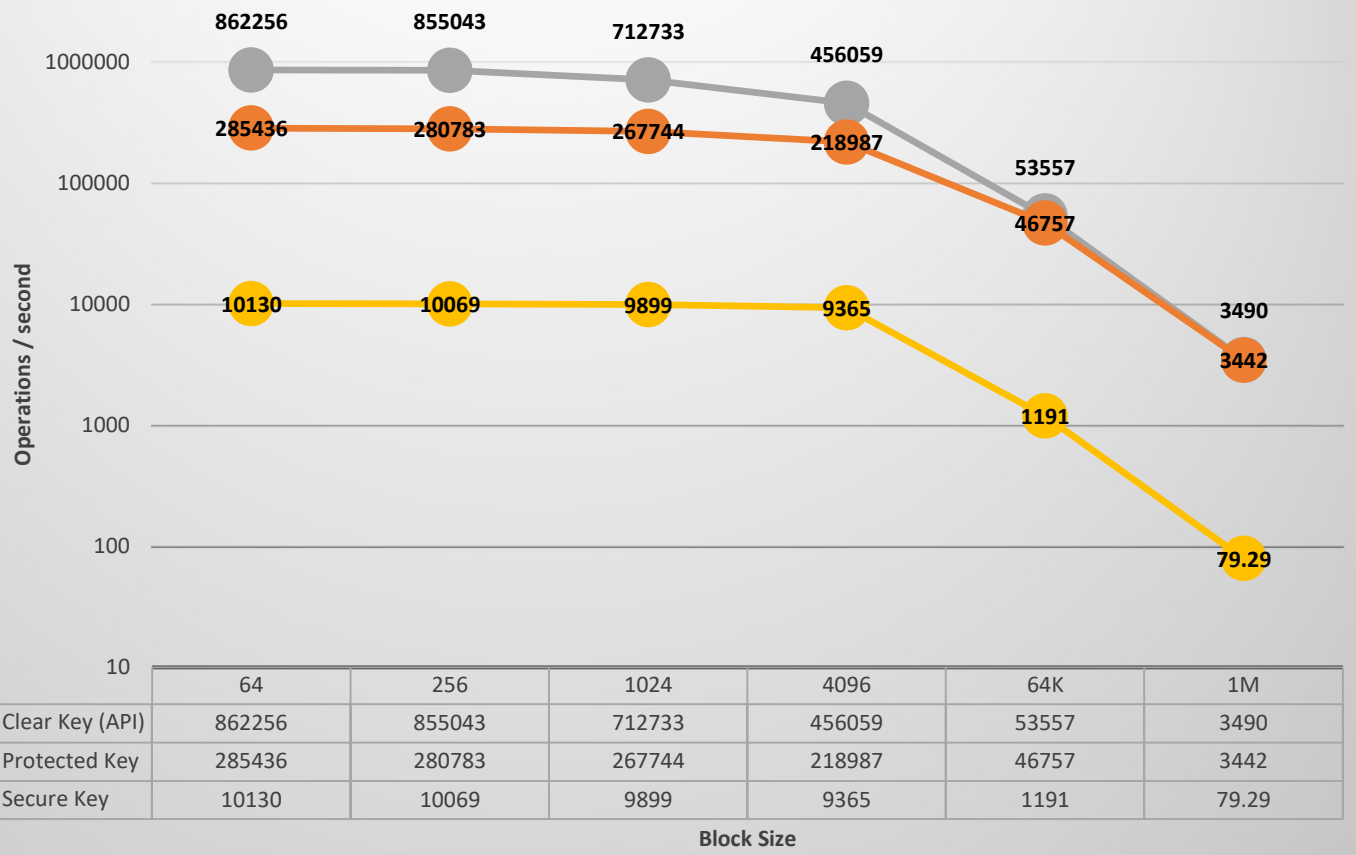




z15 Performance Metrics

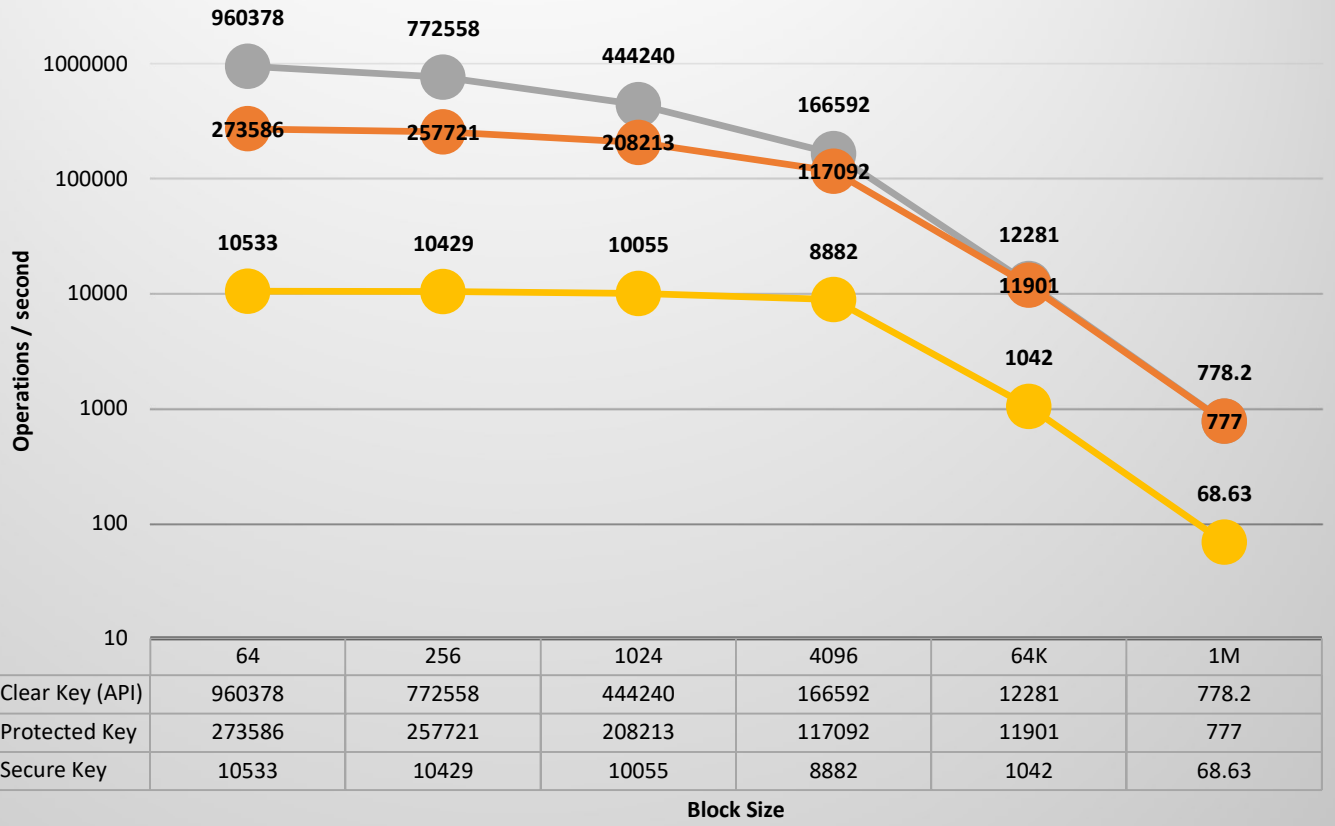
- IBM z15 Performance of Cryptographic Operations
  (Cryptographic Hardware: CPACF, CEX7S)
  - https://www.ibm.com/downloads/cas/6K2653EJ
  - Or Google ‘z15 Performance of Cryptographic Operations’

Compare Clear, Protected, Secure Key
AES CBC w/256-bit Key



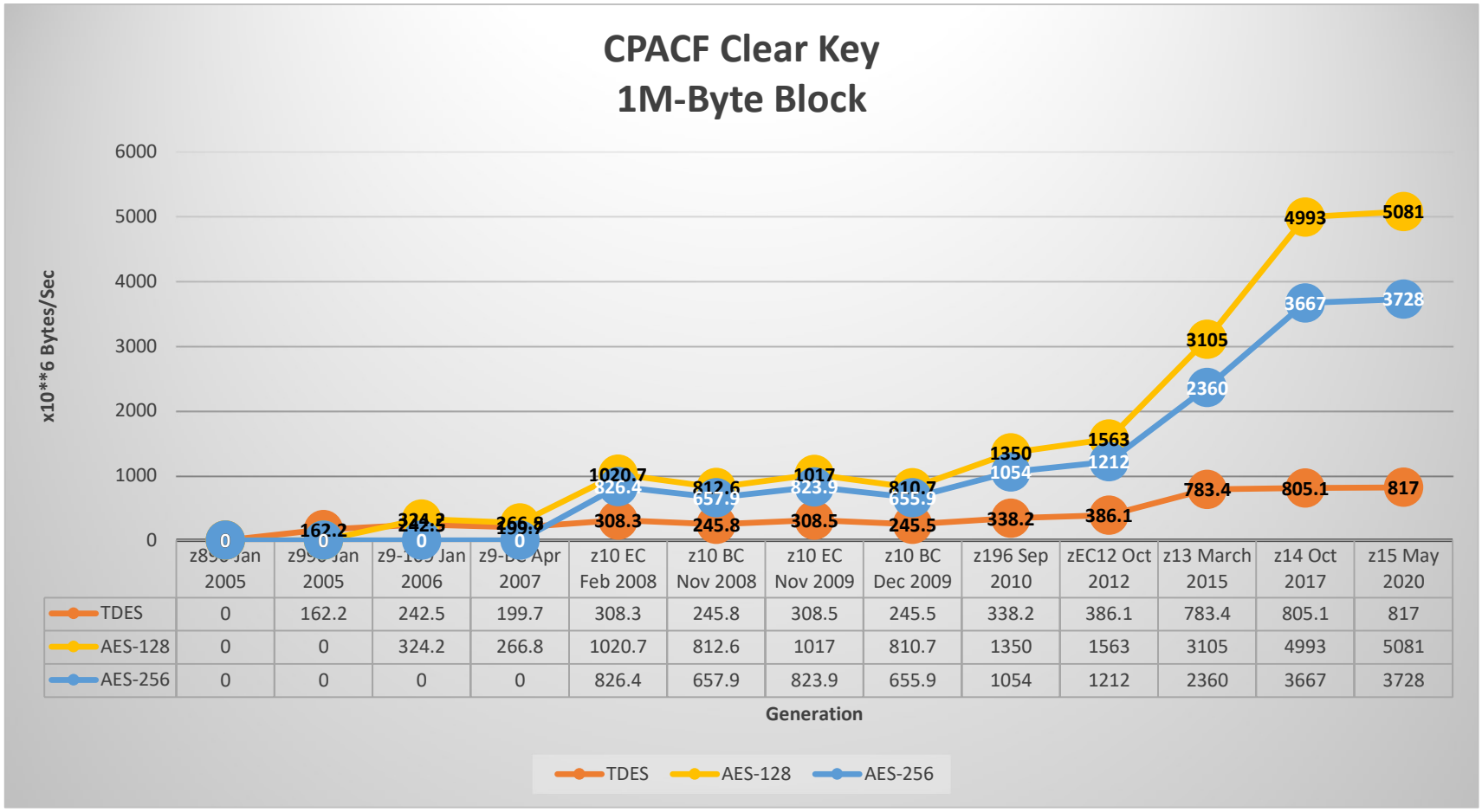
	64	256	1024	4096	64K	1M
AES Clear Key (API)	862256	855043	712733	456059	53557	3490
AES Protected Key	285436	280783	267744	218987	46757	3442
AES Secure Key	10130	10069	9899	9365	1191	79.29

Compare Clear, Protected, Secure Key
DES CBC w/TDES Key



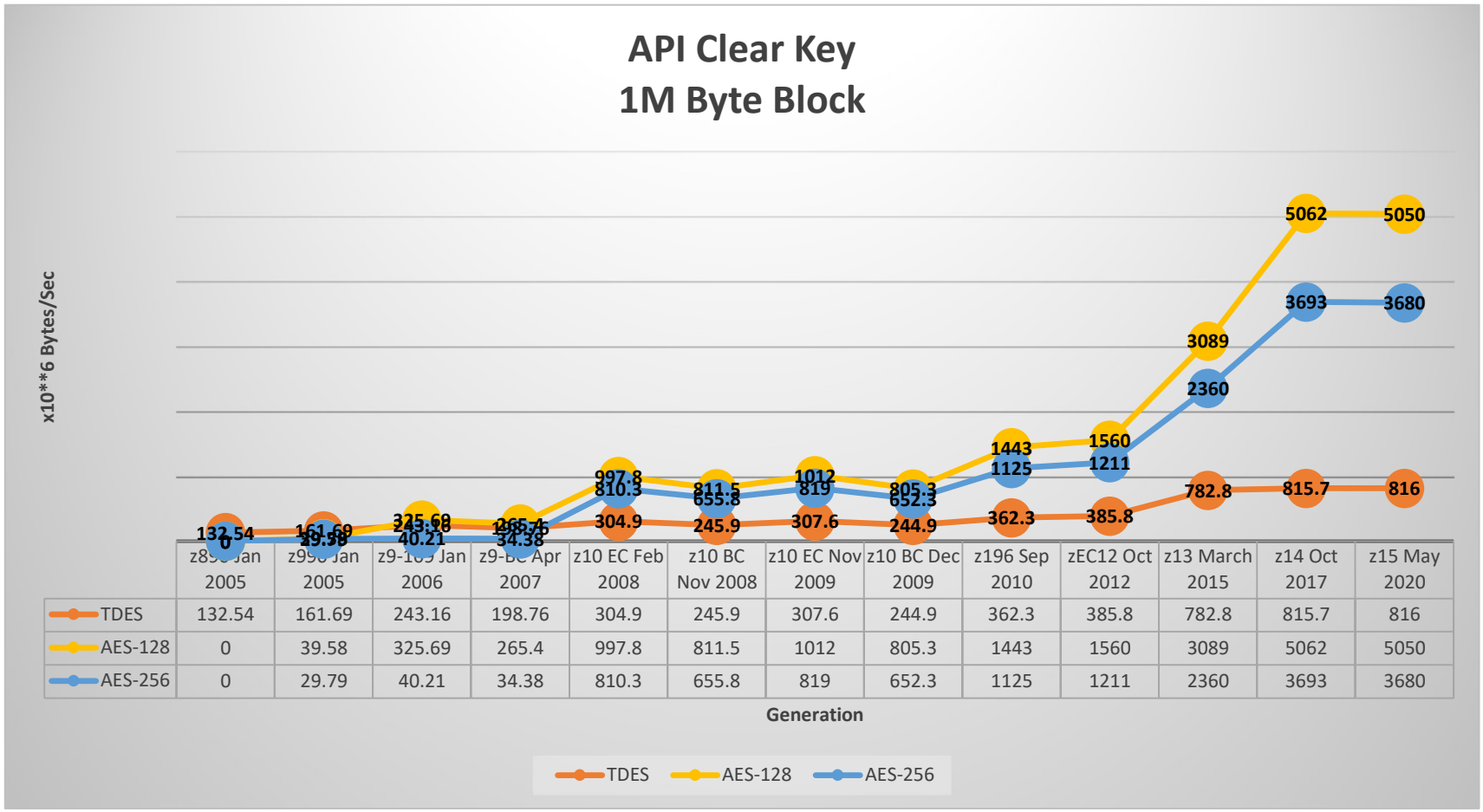
	64	256	1024	4096	64K	1M
TDES Clear Key (API)	960378	772558	444240	166592	12281	778.2
TDES Protected Key	273586	257721	208213	117092	11901	777
TDES Secure Key	10533	10429	10055	8882	1042	68.63

Crypto performance across CECs - CPACF



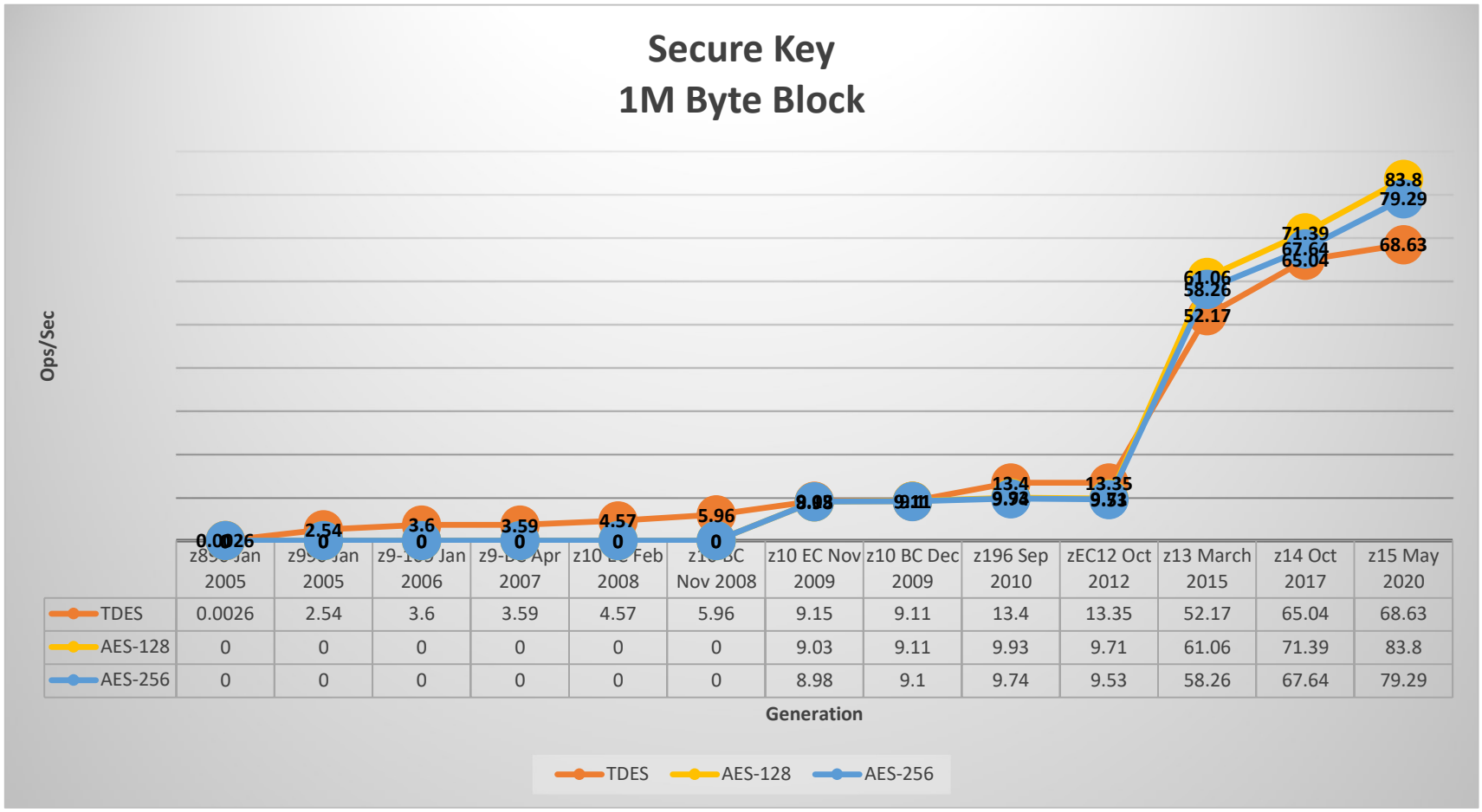
	z890 Jan 2005	z990 Jan 2005	z9-109 Jan 2006	z9-BC Apr 2007	z10 EC Feb 2008	z10 BC Nov 2008	z10 EC Nov 2009	z10 BC Dec 2009	z196 Sep 2010	zEC12 Oct 2012	z13 March 2015	z14 Oct 2017	z15 May 2020
TDES	0	162.2	242.5	199.7	308.3	245.8	308.5	245.5	338.2	386.1	783.4	805.1	817
AES-128	0	0	324.2	266.8	1020.7	812.6	1017	810.7	1350	1563	3105	4993	5081
AES-256	0	0	0	0	826.4	657.9	823.9	655.9	1054	1212	2360	3667	3728

Crypto performance across CECs - CPACF



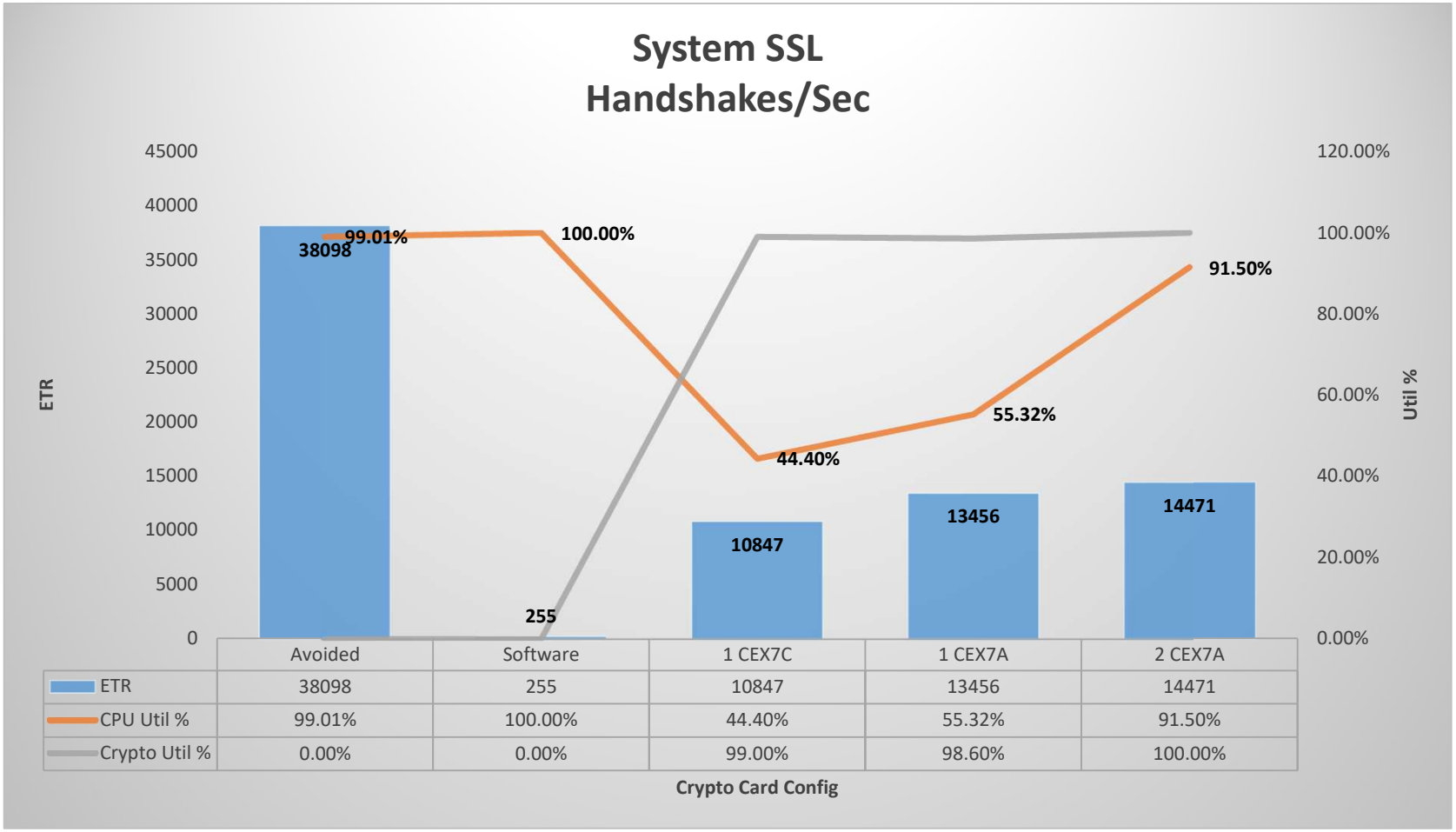
	z890 Jan 2005	z990 Jan 2005	z9-109 Jan 2006	z9-BC Apr 2007	z10 EC Feb 2008	z10 BC Nov 2008	z10 EC Nov 2009	z10 BC Dec 2009	z196 Sep 2010	zEC12 Oct 2012	z13 March 2015	z14 Oct 2017	z15 May 2020
TDES	132.54	161.69	243.16	198.76	304.9	245.9	307.6	244.9	362.3	385.8	782.8	815.7	816
AES-128	0	39.58	325.69	265.4	997.8	811.5	1012	805.3	1443	1560	3089	5062	5050
AES-256	0	29.79	40.21	34.38	810.3	655.8	819	652.3	1125	1211	2360	3693	3680

Crypto performance across CECs - CPACF



	z8[illegible] Jan 2005	z9[illegible] Jan 2005	z9-[illegible] Jan 2006	z9-[illegible] Apr 2007	z10 [illegible] Feb 2008	z10 [illegible] BC Nov 2008	z10 EC Nov 2009	z10 BC Dec 2009	z196 Sep 2010	zEC12 Oct 2012	z13 March 2015	z14 Oct 2017	z15 May 2020
TDES	0.0026	2.54	3.6	3.59	4.57	5.96	9.15	9.11	13.4	13.35	52.17	65.04	68.63
AES-128	0	0	0	0	0	0	9.03	9.11	9.93	9.71	61.06	71.39	83.8
AES-256	0	0	0	0	0	0	8.98	9.1	9.74	9.53	58.26	67.64	79.29

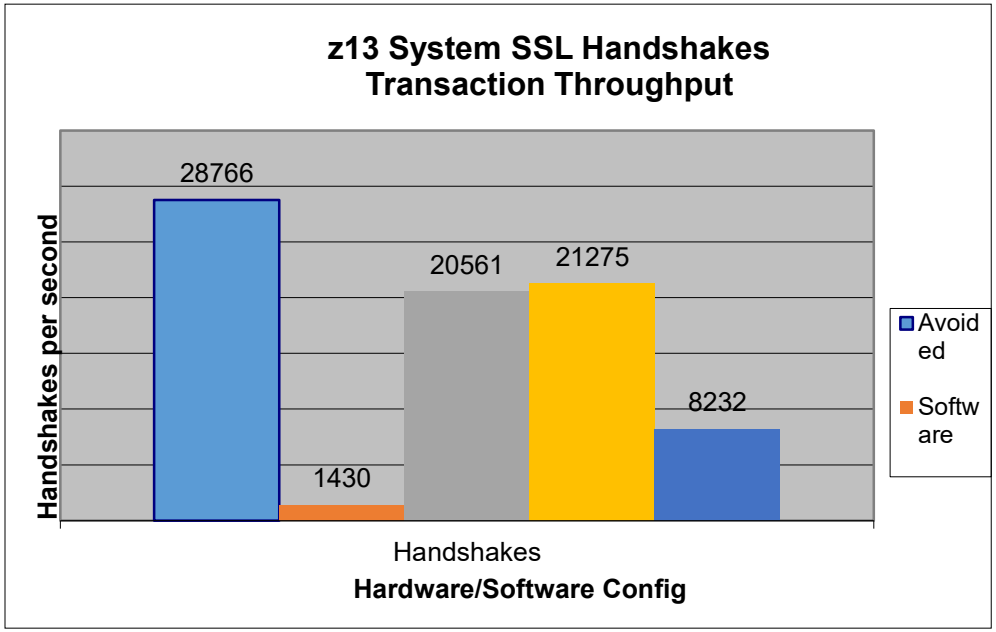
System SSL Performance – z15



IBM z15 Model 8561-770 (4 CPs)

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

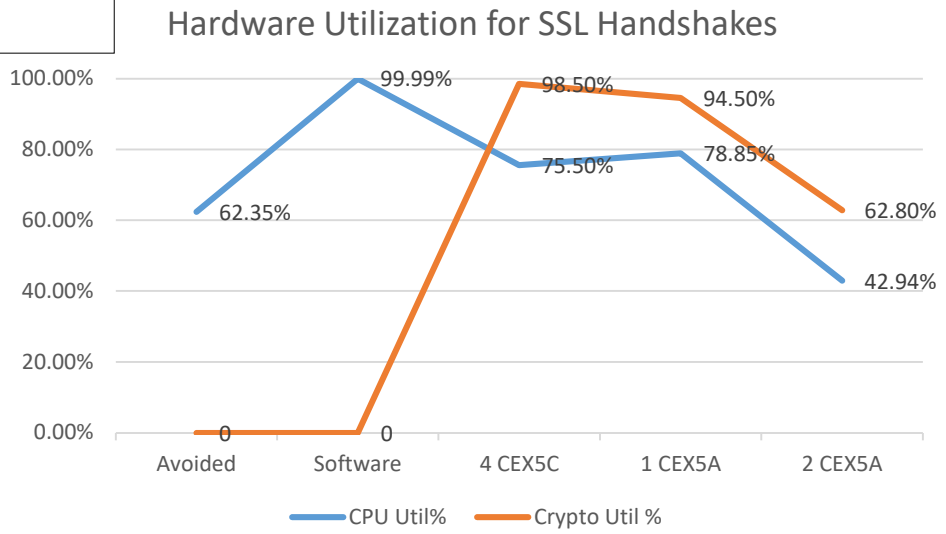
System SSL Performance – z13



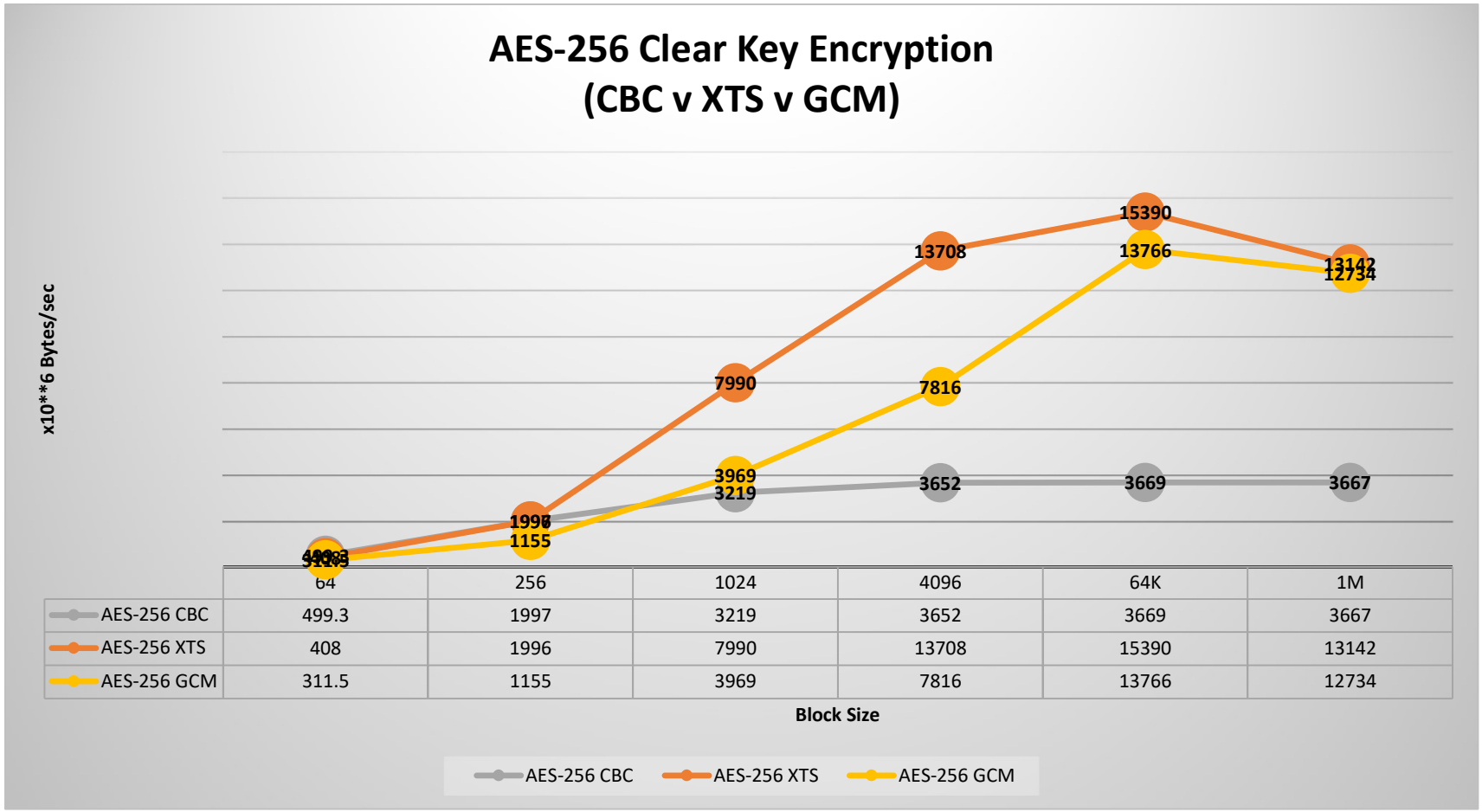
Caching SID/Client Authenti-cation	Hand-shakes	ETR	CPU Util%	Crypto Util %
100%/No	Avoided	28766	62.35%	NA
No/No	Software	1430	99.99%	NA
No/No	4 CEX5C	20561	75.50%	98.50%
No/No	1 CEX5A	21275	78.85%	94.50%
No/Yes	2 CEX5A	8232	42.94%	62.80%

IBM z13 Model 2964-N96 (4 CPs)

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

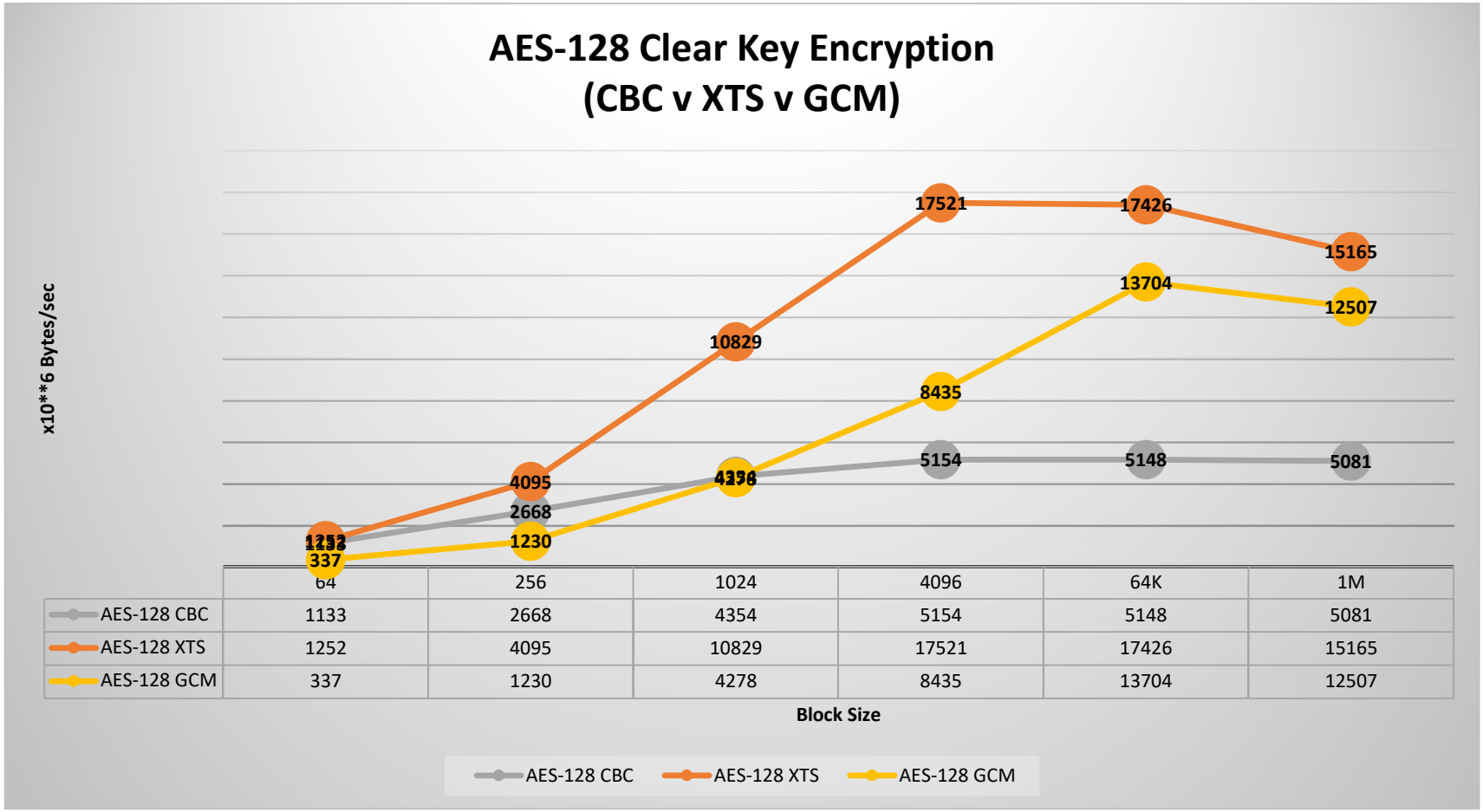


z14 Crypto Performance

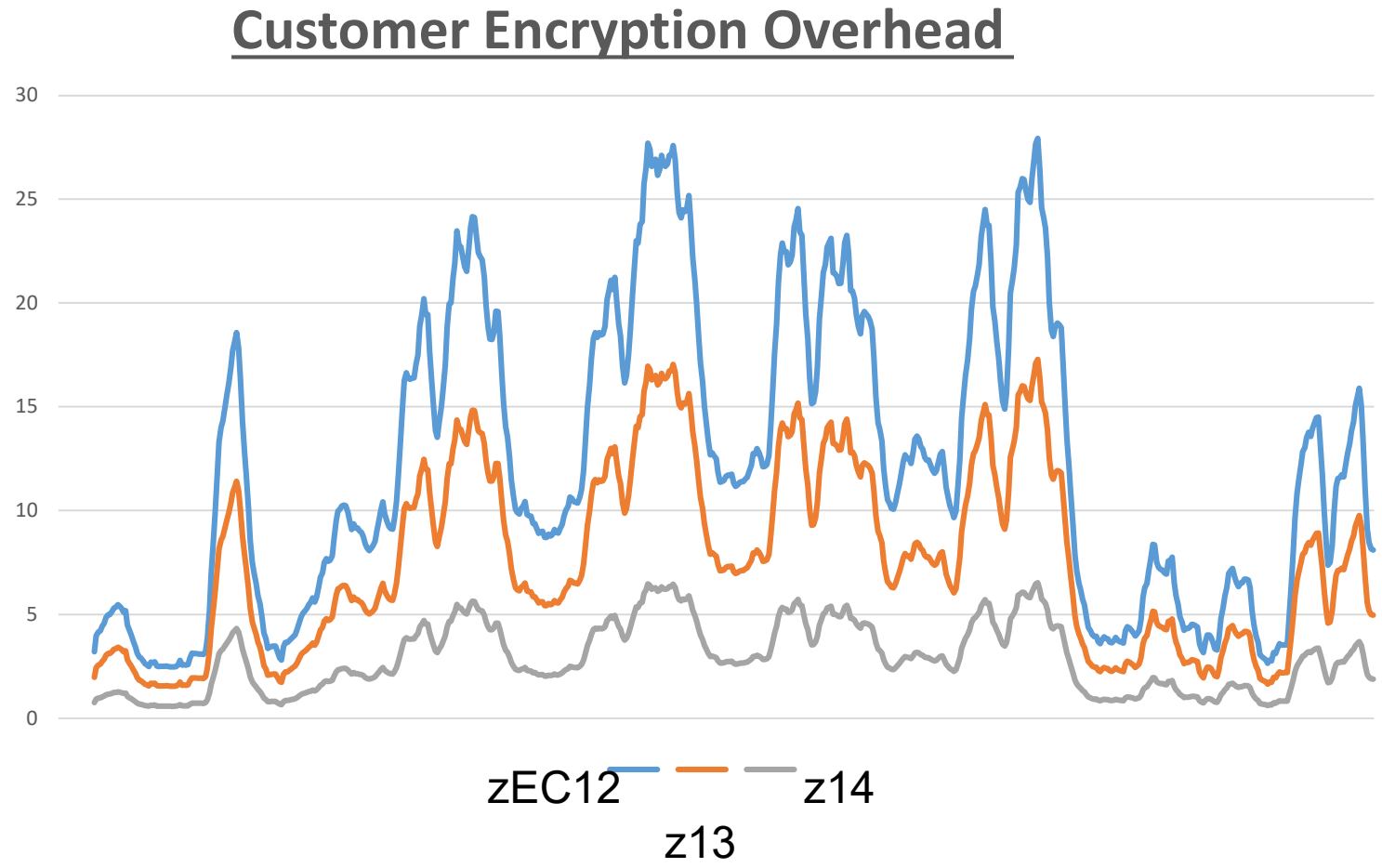


	64	256	1024	4096	64K	1M
AES-256 CBC	499.3	1997	3219	3652	3669	3667
AES-256 XTS	408	1996	7990	13708	15390	13142
AES-256 GCM	311.5	1155	3969	7816	13766	12734

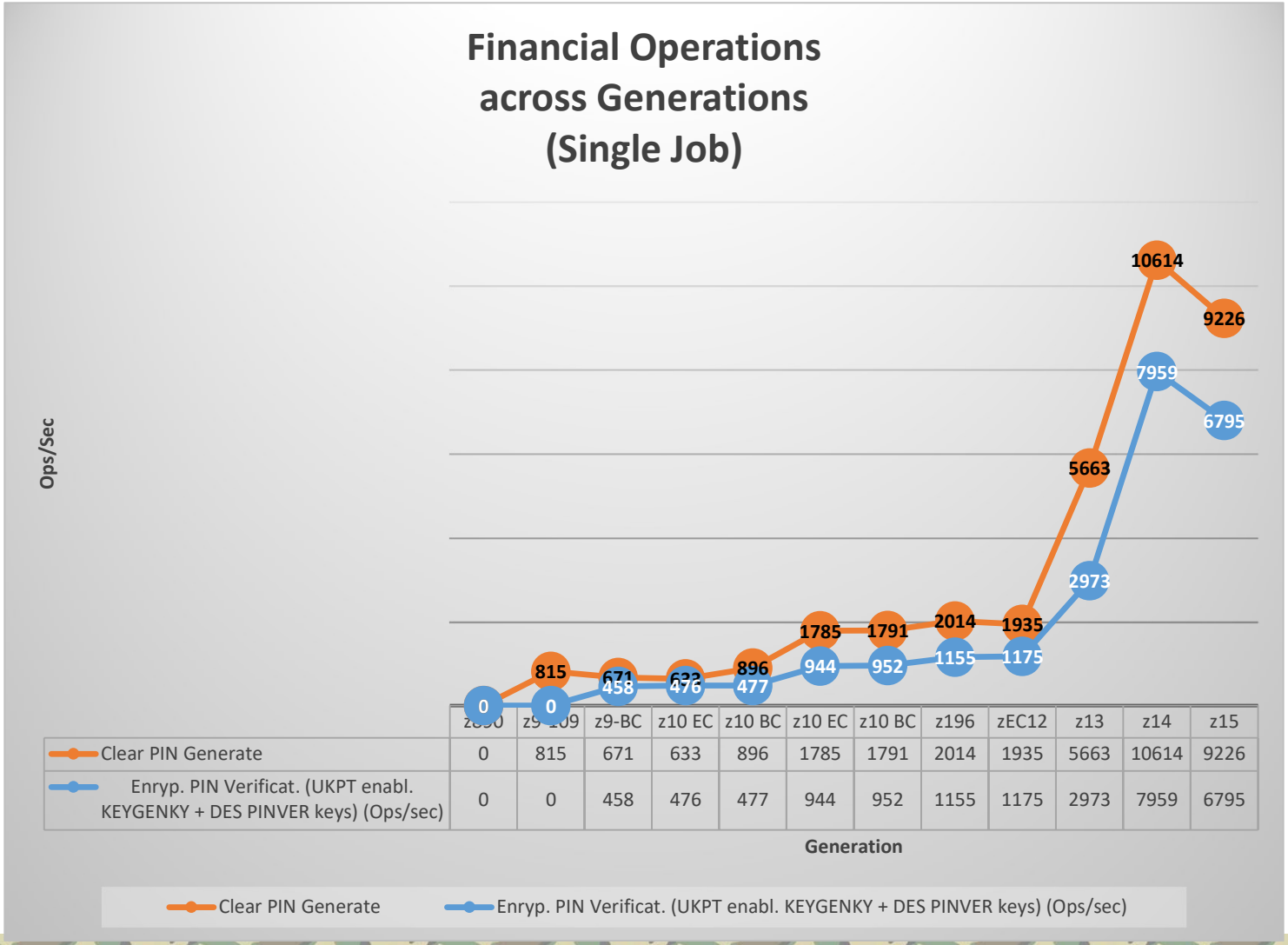
z15 Crypto Performance



4-Hour Rolling Average

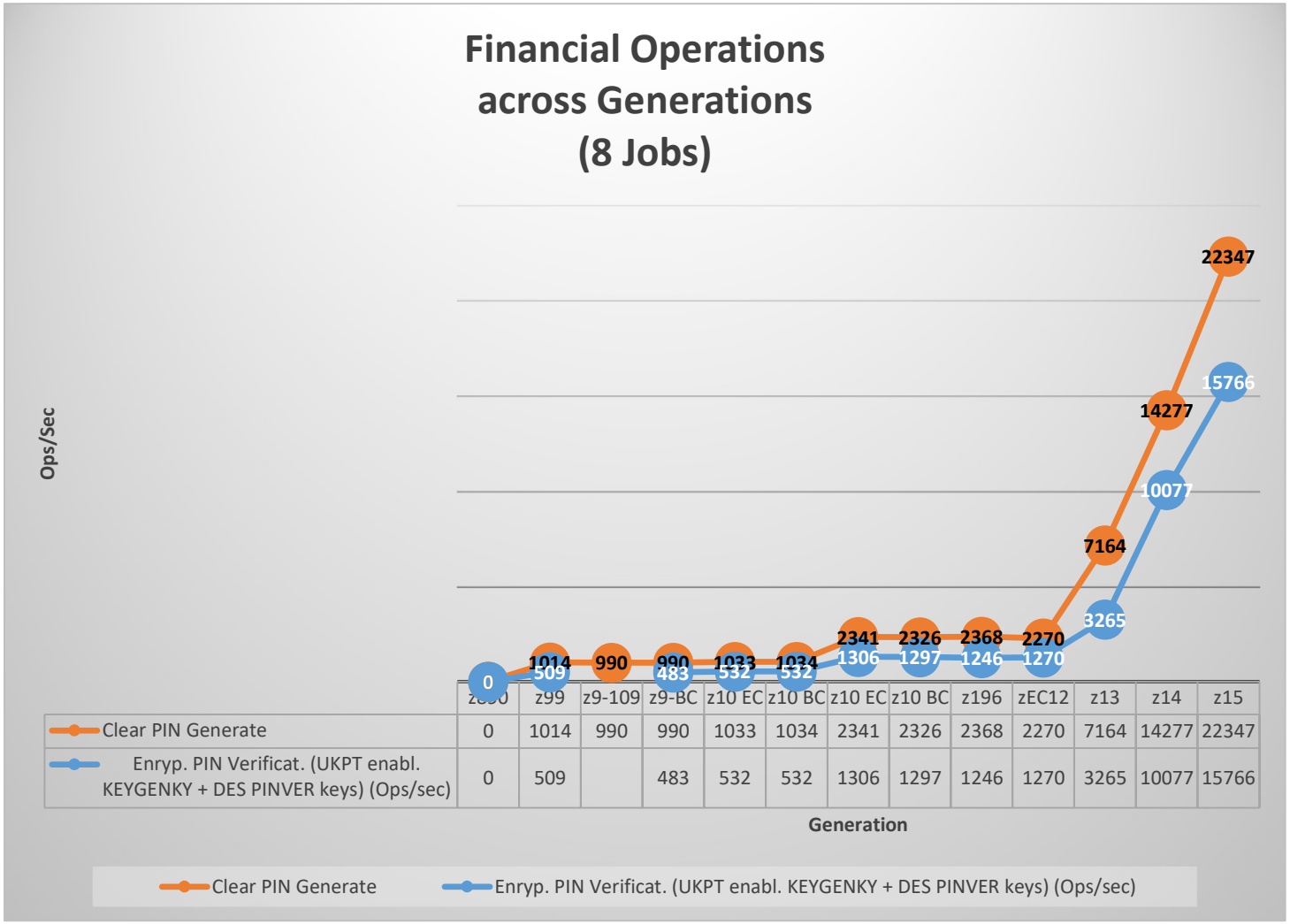


Crypto Performance across CECs – selected APIs



	z9-BC	z10 EC	z10 BC	z10 EC	z10 BC	z196	zEC12	z13	z14	z15
Clear PIN Generate	0	815	671	633	896	1785	1791	2014	1935	5663	10614	9226
Enryp. PIN Verificat. (UKPT enabl. KEYGENKY + DES PINVER keys) (Ops/sec)	0	0	458	476	477	944	952	1155	1175	2973	7959	6795

Crypto Performance across CECs – selected APIs



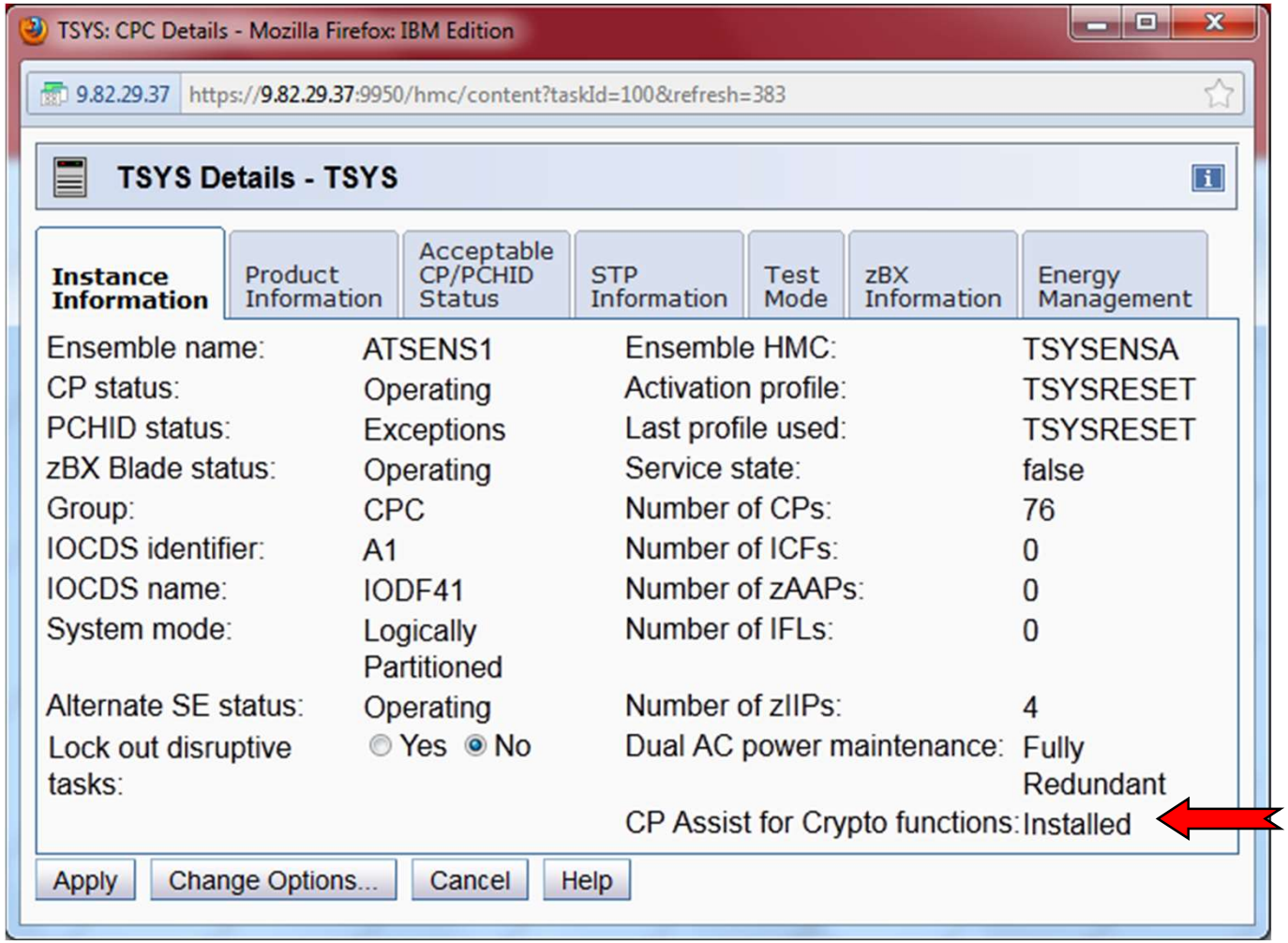
	z990	z99	z9-109	z9-BC	z10 EC	z10 BC	z10 EC	z10 BC	z196	zEC12	z13	z14	z15
Clear PIN Generate	0	1014	990	990	1033	1034	2341	2326	2368	2270	7164	14277	22347
Enryp. PIN Verificat. (UKPT enabl. KEYGENKY + DES PINVER keys) (Ops/sec)	0	509		483	532	532	1306	1297	1246	1270	3265	10077	15766

Config for Performance

- ICSF Options
  - CHECKAUTH(YES/NO) – skip SAF checks for Supervisor State or System Key callers
- Disable OWH and RNG SAF checks*
  - CSF.CSFSERV.AUTH.CSFOWH.DISABLE
  - CSF.CSFSERV.AUTH.CSFRNG.DISABLE
- RNGCACHE(YES/NO) – Take the default to use a cache for random numbers
- KDSREFDAYS(1) – Take the default to only update the header once a day

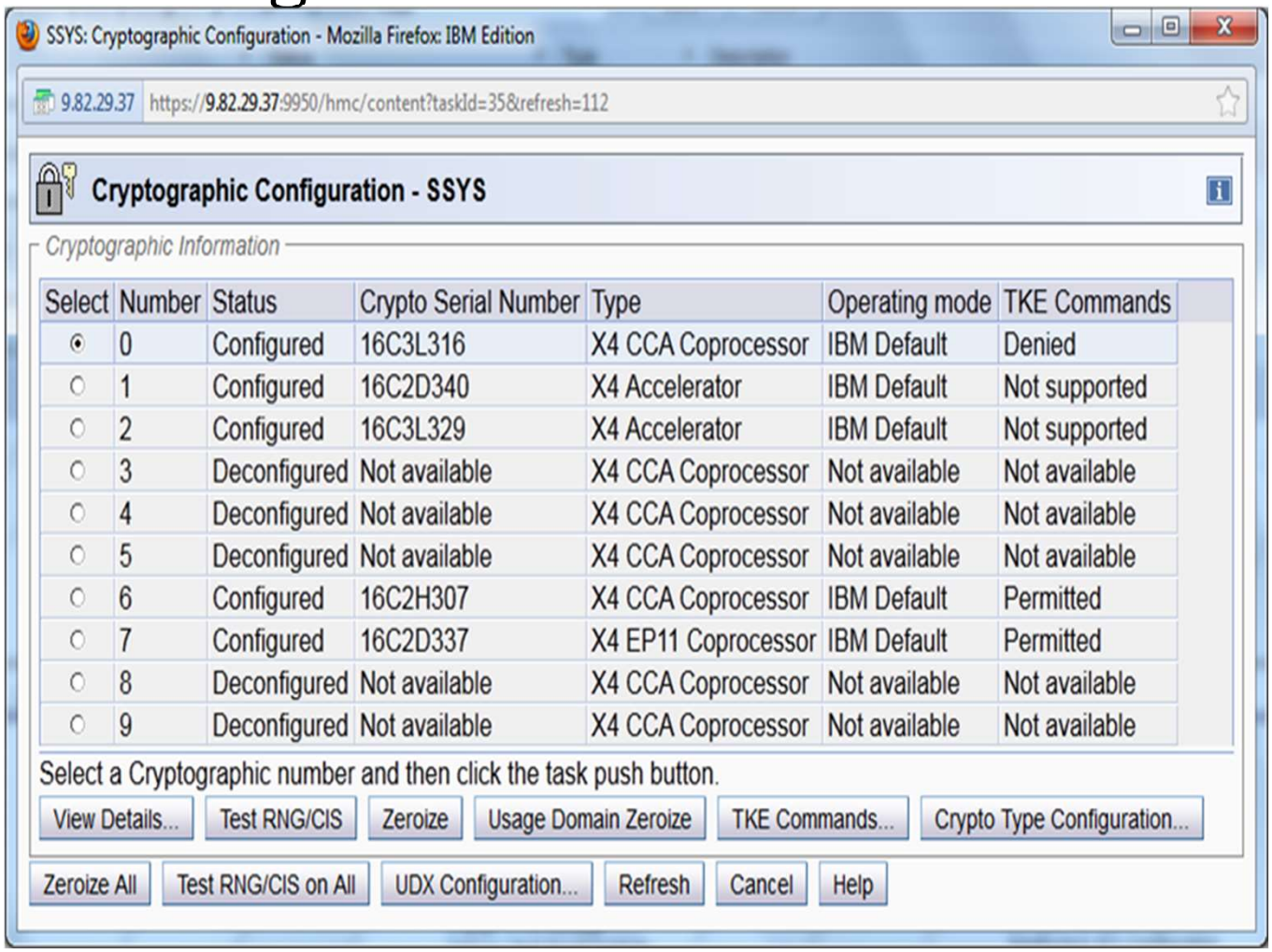
*OWH & RNG SAF Check Security Policies available in HCR77A1

Crypto Microcode Installed?



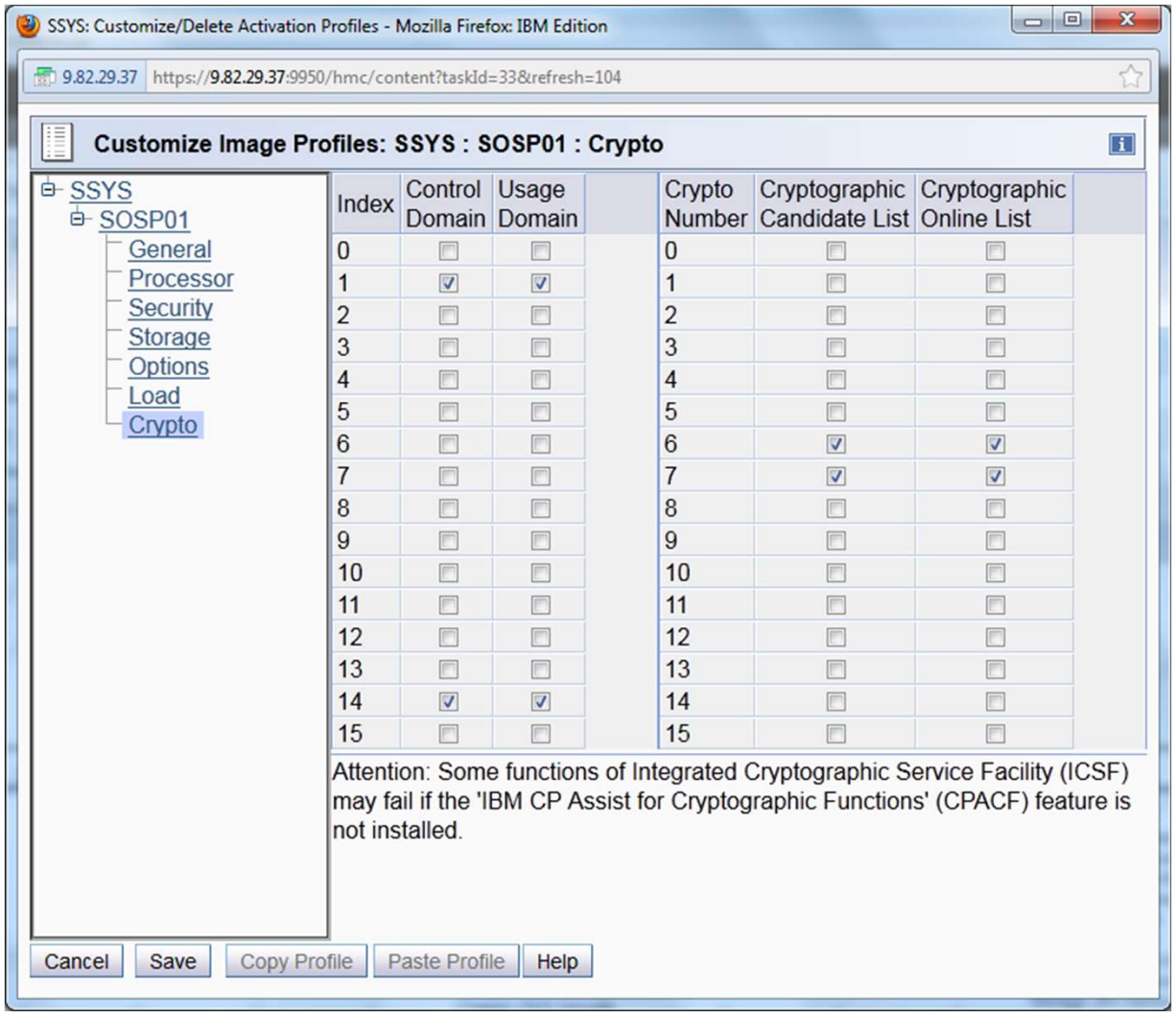
- From the HMC, in Single Object Mode, look at the CPC Details

PCI Cards Installed? And how are they configured?



From HMC, CPC Operational Customization, View LPAR Cryptographic Controls

PCI Card LPAR Assignment



Are your Master Keys loaded and correct?

	CoProcessor	Serial Number	Status	AES	DES	ECC	RSA	P11
__	G01	00000001	ONLINE	U	U	C	U	
__	G02	00000002	ACTIVE	A	U	A	E	
__	G03	00000003	ACTIVE	A	U	A	C	
__	H07		ACTIVE					
__	SC06	00000006	ACTIVE	A	U	A	C	
__	SP07	00000008	ACTIVE					A

How do I tell, what ciphersuites – F GSKSRVR,DISPLAY CRYPTO

GSK01009I Cryptographic status

Algorithm	Hardware	Software
DES	56	56
3DES	168	168
AES	256	256
RC2	--	128
RC4	--	128
RSA Encrypt	--	4096
RSA Sign	--	4096
DSS	--	1024
SHA-1	160	160
SHA-2	512	512
ECC	--	--

Environment: z196 running z/OS 1.13, but ICSF not active

How do I tell, what ciphersuites – F GSKSRVR,DISPLAY CRYPTO

GSK01009I Cryptographic status

Algorithm	Hardware	Software
DES	56	56
3DES	168	168
AES	256	256
RC2	--	128
RC4	--	128
RSA Encrypt	4096	4096
RSA Sign	4096	4096
DSS	--	1024
SHA-1	160	160
SHA-2	512	512
ECC	521	521

Environment: z196 running z/OS 1.13, with ICSF active

CPU Measurement Facility

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

*New on z15

Counter #	Description	Counter #	Description
64	Pseudo RNG Function Count	65	Pseudo RNG Cycle Count
66	Pseudo RNG Blocked Function Count	67	Pseudo RNG Blocked Cycle Count
68	SHA Function Count	69	SHA Cycle Count
70	SHA Blocked Function Count	71	SHA Blocked Cycle Count
72	DEA Function Count	73	DEA Cycle Count
74	DEA Blocked Function Count	75	DEA Blocked Cycle Count
76	AES Function Count	77	AES Cycle Count
78	AES Blocked Function Count	79	AES Blocked Cycle Count
80*	ECC function count	81*	ECC cycle count
82*	ECC blocked function count	83*	ECC blocked cycle count

SMF Type 82 – ICSF Record

- **Subtype 1 – Initialization options**
- **Subtype 7 – Operational key load**
- **Subtype 8 – Cryptographic key data set refresh**
- **Subtype 9 – Dynamic CKDS Update**
- **Subtype 13 – Dynamic PKDS update**
- **Subtype 14 – Cryptographic coprocessor master key entry**
- **Subtype 15 – PCI Crypto copr retained key create/delete**
- **Subtype 16 – PCI Cryptographic coprocessor TKE**
- **Subtype 18 – Cryptographic processor configuration**
- **Subtype 19 – PCI X Cryptographic coprocessor timing**
- **Subtype 20 – Cryptographic processor processing times**
- **Subtype 21 – ICSF Sysplex group change**

SMF Type 82 – ICSF Record (cont.)

- **Subtype 22 – Trusted block create callable services**
- **Subtype 23 – Token data set update**
- **Subtype 24 – Duplicate tokens found**
- **Subtype 25 – Key store policy for key token auth checking**
- **Subtype 26 – Public key data set refresh**
- **Subtype 27 – PKA key management extensions**
- **Subtype 28 – High performance encrypted key (Protected Key)**
- **Subtype 29 – TKE workstation audit record**
- **Subtype 30 – Key store policy archived & inactive KDS records**

SMF Type 82 – ICSF Record (cont.)

- **Subtype 31 – Cryptographic usage statistics**
- **Subtype 40 – CCA symmetric key lifecycle event**
- **Subtype 41 – CCA asymmetric key lifecycle event**
- **Subtype 42 – PKCS #11 object lifecycle event**
- **Subtype 43 – Regional cryptographic server configuration**
- **Subtype 44 – CCA symmetric key usage event**
- **Subtype 45 –CCA asymmetric key usage event**
- **Subtype 46 – PKCS #11 key usage event**
- **Subtype 47 – PKCS #11 no key usage event**
- **Subtype 48 – Compliance warning event**
- **Subtype 49 – Master key event resulted in a new master key value being promoted to current**

REXX EXEC CSFSMFR

- Formats the SMF Type 82 records into a readable report
  - Sample Job, CSFSMFJ to
    - Capture the Type 82 records (with IFASMFDP)
    - Sort the records
    - Execute CSFMFR, via Batch TSO
  - Output may be large – multiple lines per Type 82 record
  - It's more readable than the raw SMF record, but still a bit complex

Type 82, Subtype 20

Subtype=0014 Cryptographic Processor Timing

Written periodically to provide some indication of coprocessor and accelerator usage

6 Jul 2016 8:57:08.39

TME... 00312D37 DTE... 0116188F SID... S1 SSI... 00000000 STY... 0014

TFL... 04000002

04------ Coprocessor is a CEX4 or higher

------02 Configured as a CCA coprocessor

TNQ... D10076427E08A61A TDQ...D10076427EB5EF18 TWT...D10076427EB61018

Offsets		Field Name	Length	Format	Description
4	4	SMF82TNQ	8	EBCDIC	Coprocessor time before NQAP
12	C	SMF82TDQ	8	EBCDIC	Coprocessor time after DQAP
20	14	SMF82TWT	8	EBCDIC	Coprocessor time after WAIT
28	1C	SMF82TQU	4	Binary	Coprocessor queue length

Monitoring Crypto Operations (HCR77C1)

- ICSF Options
  - STATS(…,…,…)
    - ENG – track cryptographic engines
    - SRV – track cryptographic services
    - ALG – track cryptographic algorithms
  - STATSFILTER – level of aggregation (for high volume apps)
- SMF Type 82 Subtype 31
  - The jobs and tasks that are using the various cryptographic engines.
  - The cryptographic card types that are getting the most requests.
  - If any cryptographic requests are being handled in software.
  - The peak periods of cryptographic usage.
  - The ICSF services that are being started by other z/OS components.
  - The jobs and tasks that are using out-of-date algorithms or key sizes.

Cryptographic Key Usage Statistics

```
Subtype=001F Crypto Usage Statistics
Written periodically to record crypto usage counts
7 Mar 2018 11:30:30.00
  TME... 003F3798 DTE... 0118066F SID... MFC1     SSI... 00000000 STY... 001F
  INTVAL_START.. 03/07/2018 16:20:30.000330
  INTVAL_END.... 03/07/2018 16:30:30.000548
  USERID_AS..... GBOYD
  USERID_TK.....
  JOBID......... TSU13812
  JOBNAME....... BOYDG
  JOBNAME2......
  PLEXNAME...... MFCPLEX
  DOMAIN........ 12
  ENG...CARD...5C01/DV53K342... 50
  ENG...CARD...5C03/DV53G424... 50
  ENG...CPACF... 100
  ALG...AES256..... 200
  SRV...CSFSYE..... 100
  SRV...CSFSAD..... 100
```

SMF Type 70, Subtype 2 - RMF Processor Activity

- Cryptographic Coprocessor Data Section
  - Processor Index, Processor Type
  - Scaling Factor
  - Execution Time of all operations
  - Number of all operations on the coprocessor
  - Number of all RSA-key-generation operations
- Cryptographic Accelerator Data Section
  - Processor Index, Processor Type
  - Validity bit mask, Number of engines on the accelerator
  - Scaling factor
  - Execution time & number of operations by
    - 1024-bit-ME 2048-bit-ME
    - 1024-bit-CRT 2048-bit-CRT
    - 4096-bit-ME 4096-bit CRT

SMF Type 70, Subtype 2 - RMF Processor Activity

- Cryptographic PKCS11 Coprocessor Data Section
  - Processor Index, Processor Type
  - Scaling Factor
  - Aggregate Execution Time, Number of Operations
    - Slow asymmetric-key functions
    - Fast asymmetric-key functions
    - Asymmetric-key generation
    - Symmetric-key functions complete
    - Symmetric-key functions partial

SMF Type 70, Subtype 2 - RMF Processor Activity (cont.)

- ICSF Services Data Section
  - Single DES (Encipher & Decipher): Number of calls, bytes, and instructions
  - Triple DES (Encipher & Decipher): Number of calls, bytes, and instructions
  - MAC Generate/Verify: Number of calls to generate/verify, number of bytes for which MAC was generated/verified, number of PCMF instructions used to generate/verify the MAC
  - SHA-1: Number of calls to hash, number of bytes that were hashed, number of PCMF instructions used to hash the data
  - PIN: number of translate calls, number of verify calls
  - SHA-224, SHA-256, SHA-384, SHA-512 : Number of calls to hash, number of bytes that was hashed, number of PCMF instructions used to hash the data
  - ICSF Data Level
  - AES Encipher & Decipher: number of calls sent to cop, number of bytes processed, number of operations

RMF Crypto Hardware Activity Report

(From z/OS RMF Report Analysis 2.4, SC34-2665-40)

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 V2R3 SYSTEM ID TRX2 DATE 02/01/2017 INTERVAL 14.59.998
RPT VERSION V2R3 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

(From z/OS RMF Report Analysis 2.4, SC34-2665-40)

-------- 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

(From z/OS RMF Report Analysis 2.4, SC34-2665-40)

-------- 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 ME1024				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

(From z/OS RMF Report Analysis 2.4, SC34-2665-40)

-------- 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

SMF Type 70 Subtype 2 – RMF Processor Activity

RMF Monitor III

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

CRYOVW – Crypto Hardware Overview Report

RMF V2R4 Crypto HW Overview - ENGTEST3 Line 1 of 22
Samples: 100 Systems: 4 Date: 02/14/19 Time: 06.00.00 Range: 100 Sec

Type	ID	--CPC---	-System-	Rate	Exec Time	Util%	----- Key Gen ----- Rate	ExTime	Util%
CEX5C	0	M88		6223	0.160	99.7	0.730	0.191	0.0
CEX5C	0	M88	S24	66.46	0.146	1.0	0.000	0.000	0.0
CEX5C	0	M88	S25	6157	0.160	98.7	0.730	0.191	0.0
CEX5P	3	M88		949.4	1.053	100			
CEX5P	3	M88	S24	280.5	1.102	30.9			
CEX5P	3	M88	S25	668.9	1.032	69.0			
CEX6A	9	M88		5237	0.195	100			
CEX6A	9	M88	S24	2486	0.012	2.9			
CEX6A	9	M88	S25	2751	0.361	99.4			
CEX6C	12	M88		6111	0.163	99.7	0.030	0.127	0.0
CEX6C	12	M88	S24	317.7	0.269	8.5	0.000	0.000	0.0
CEX6C	12	M88	S25	5793	0.157	91.1	0.030	0.127	0.0
CEX4C	1	P88		468.8	0.706	33.1	0.000	0.000	0.0
CEX3C	4	P88		465.0	0.685	31.8	0.000	0.000	0.0
CEX3A	5	P88		5472	0.129	70.8			
CEX4P	13	P88		28.19	12.22	34.5			
CEX4C	14	P88		460.6	0.688	31.7	0.000	0.000	0.0
CEX4P	15	P88		26.62	12.65	33.7			
CEX5P	4	S89		826.4	0.923	76.3			
CEX5P	5	S89		827.1	0.919	76.0			
CEX5C	6	S89		1219	0.820	99.9	0.000	0.000	0.0
CEX5A	9	S89		820.8	1.218	100			

CRYACC – Crypto Accelerator Activity Report

RMF V2R4 Crypto Acc Activity - ENGTEST3 Line 1 of 15

Samples: 100 Systems: 4 Date: 02/14/19 Time: 06.00.00 Range: 100 Sec

Type	ID	--CPC---	-System-	-Key	----- ME RSA -----			---- CRT RSA -----		
				Len	Rate	ExTime	Util%	Rate	ExTime	Util%
CEX6A	9	M88		1024	2705	0.023	6.1	64.25	0.078	0.5
CEX6A	9	M88		2048	223.7	0.040	0.9	274.6	0.334	9.2
CEX6A	9	M88		4096	661.6	0.122	8.0	1308	0.593	77.6
CEX6A	9	M88	S24	1024	2486	0.012	2.9	0.000	0.000	0.0
CEX6A	9	M88	S24	2048	0.000	0.000	0.0	0.000	0.000	0.0
CEX6A	9	M88	S24	4096	0.000	0.000	0.0	0.000	0.000	0.0
CEX6A	9	M88	S25	1024	218.5	0.147	3.2	64.25	0.078	0.5
CEX6A	9	M88	S25	2048	223.7	0.040	0.9	274.6	0.334	9.2
CEX6A	9	M88	S25	4096	661.6	0.122	8.0	1308	0.593	77.6
CEX3A	5	P88		1024	0.000	0.000	0.0	5472	0.129	70.8
CEX3A	5	P88		2048	0.000	0.000	0.0	0.000	0.000	0.0
CEX3A	5	P88		4096	0.000	0.000	0.0	0.000	0.000	0.0
CEX5A	9	S89		1024	0.000	0.000	0.0	0.000	0.000	0.0
CEX5A	9	S89		2048	0.000	0.000	0.0	147.8	0.522	7.7
CEX5A	9	S89		4096	0.000	0.000	0.0	673.0	1.371	92.2

CRYPKC – Crypto PKCS11 Coprocessor Activity Report

```
    RMF V2R4     Crypto PKCS11 Act.       - ENGTEST3       Line 1 of 7

Samples: 100  Systems: 4  Date: 02/14/19 Time: 06.00.00 Range: 100 Sec
Type  ID --CPC--- -System- -Asym Slow -Asym Fast -Symm Part -Symm Cmpl
                            Rate Utl%  Rate Utl%  Rate Utl%  Rate Utl%
CEX5P  3 M88               533.7 52.6  99.1 46.6 0.000 0.0 16.07  0.7
CEX5P  3 M88       S24     231.4 21.4 40.57  9.2 0.000 0.0 8.450  0.4
CEX5P  3 M88       S2      302.3 31.2 358.5 37.4 0.000 0.0 7.620  0.3
CEX4P 13 P88               13.97  3.3 0.000  0.0 0.000 0.0 14.14 31.1
CEX4P 15 P88               13.07  3.8 0.000  0.0 0.000 0.0 12.90 29.3
CEX5P  4 S89               341.6 34.3 484.8 42.0 0.000 0.0 0.000  0.0
CEX5P  5 S89               341.8 34.3 485.3 41.7 0.000 0.0 0.000  0.0
```

RMF Overview Report – Type 70-1

OVW(ENCRMSU(LACSCR))

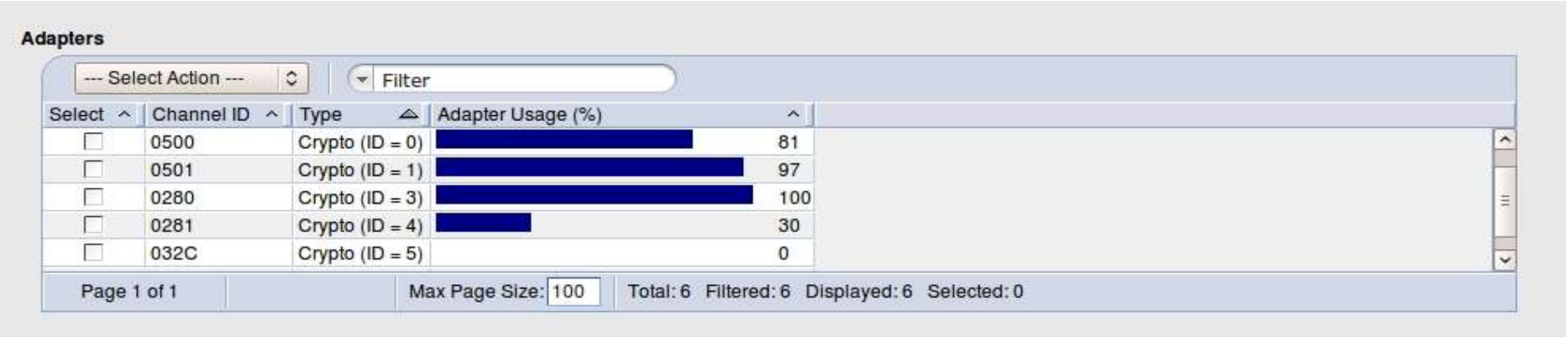
```
          R M F     O V E R V I E W
  z/OS V2R2        SYSTEM ID JA0                        START 0
      CONVERTED TO z/OS V2R3 RMF                 END 0
NUMBER OF INTERVALS 14       TOTAL LENGTH OF INTERVALS 07.00.00
    DATE     TIME         INT              ENCRMSU
    MM/DD    HH.MM.SS     HH.MM.SS
    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)

HMC Dashboard Monitor

- The HMC/SE Monitors on the zEC12 now include a display for the crypto adapters.
- The Adapter Usage percentage is the same utilization that shows up in the RMF Crypto Hardware Activity Report.
- The Utilization on the card is calculated using the formula:
  U = (Ta2 - Ta1) * S / (T2 -T1)

Ta: time used for execution S: scaling factor T: Time of measurement interval



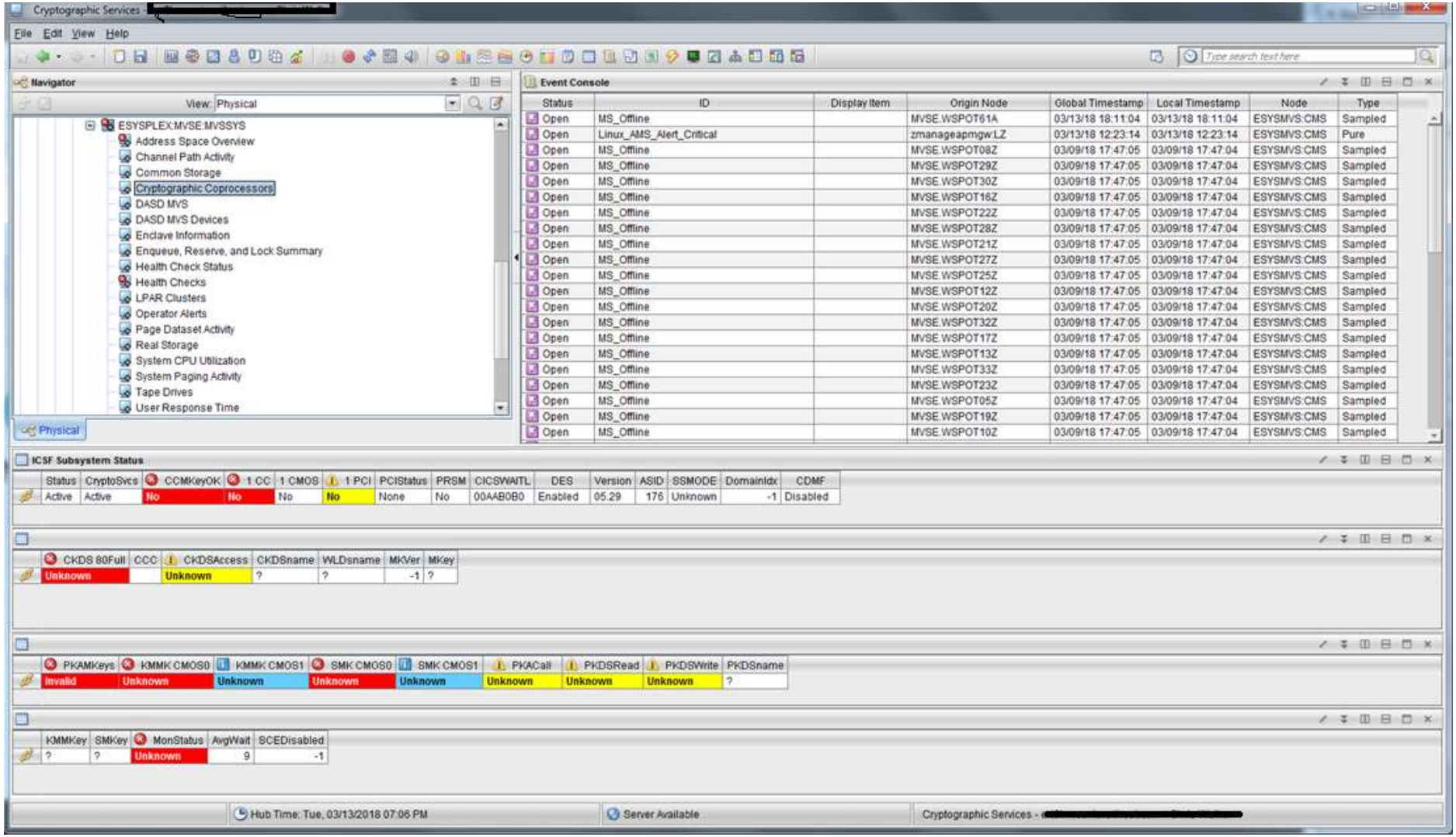
Workload Activity (SMF Type 72, Subtype 3)

- Crypto Using Samples
  - R723APU - AP crypto using samples: a TCB was found executing on a cryptographic assist processor
  - R723APD - AP crypto delay samples: a TCB was found waiting on a cryptographic assist processor

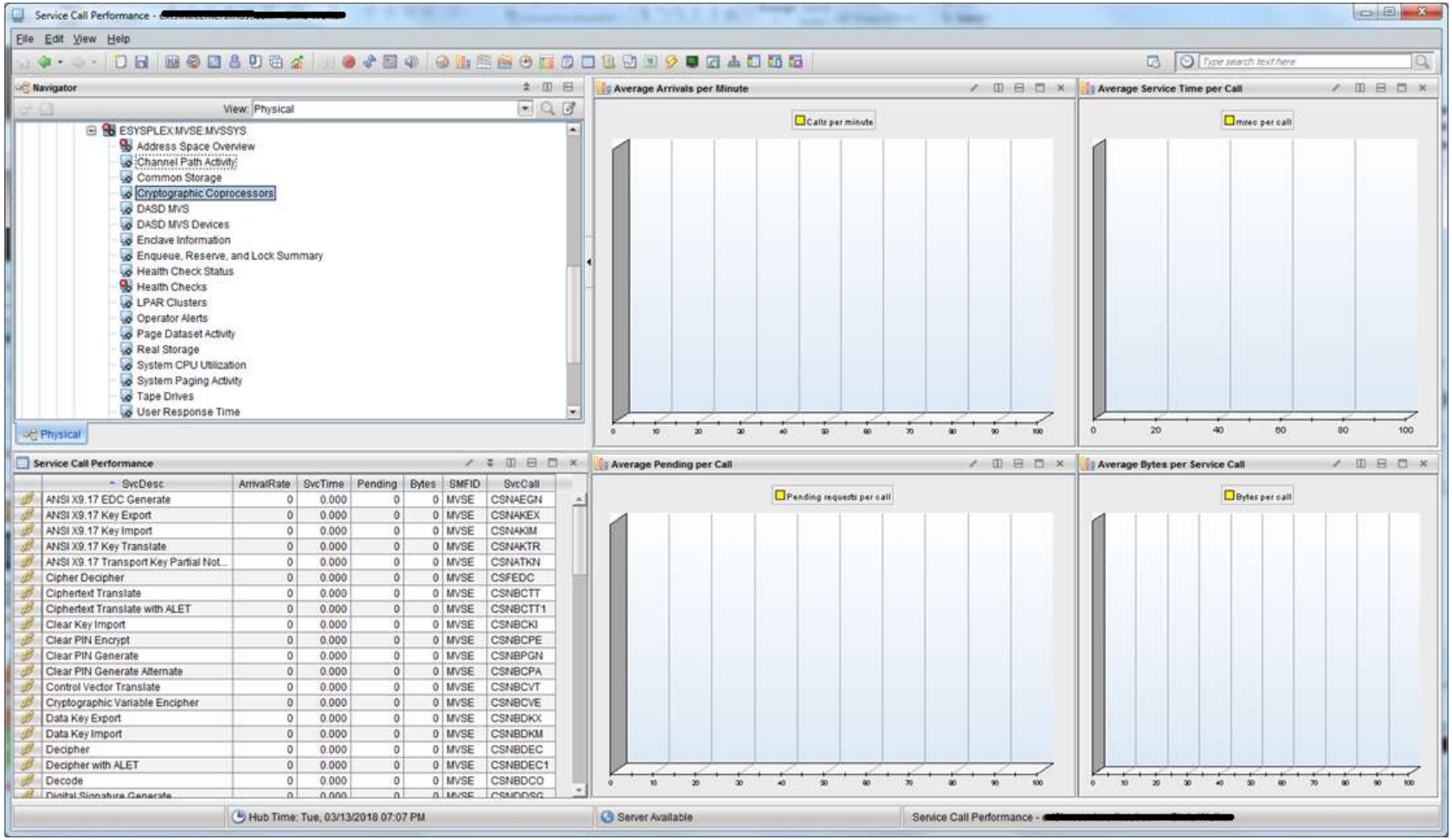
Common Address Space Work (SMF Type 30)

- SMF30CSC – ICSF Service Count
  - CSNBENC (Single-DES) - # of service calls, # of bytes, # of CMD instructions
  - CSNBENC (Double & Triple-DES) - # of service calls, # of bytes, # of CMD instructions
  - CSNBDEC (Single-DES) - # of service calls, # of bytes, # of CMD instructions
  - CSNBDEC (Double & Triple-DES) - # of service calls, # of bytes, # of CMD instructions
  - CSNBMGN (MAC Generate) - single and various double key MAC; # of service calls, # of bytes, # of CMD instructions
  - CSNBMVR (MAC Verify) - single and various double key MAC; # of service calls, # of bytes, # of CMD instructions
  - CSNBOWH (SHA-1) - # of Service calls, # of bytes, # of PCMF instructions
  - CSNBOWH (SHA-256 which includes SHA-224) - # of Service calls , # of bytes, # of PCMF instructions
  - CSNBOWH (SHA-512 which includes SHA-384) - # of Service calls , # of bytes, # of PCMF instructions
  - CSNBPTR - # of Service calls
  - CSNBPVR - # of Service calls

Omegamon


Cryptographic Services
File Edit View Help
Navigator
View: Physical
ESYSPLEX:MVSE:MVSSYS
Address Space Overview
Channel Path Activity
Common Storage
Cryptographic Coprocessors
DASD MVS
DASD MVS Devices
Enclave Information
Enqueue, Reserve, and Lock Summary
Health Check Status
Health Checks
LPAR Clusters
Operator Alerts
Page Dataset Activity
Real Storage
System CPU Utilization
System Paging Activity
Tape Drives
User Response Time
Physical
Event Console
Status ID Display Item Origin Node Global Timestamp Local Timestamp Node Type
Open MS_Offline MVSE.WSPOT61A 03/13/18 18:11:04 03/13/18 18:11:04 ESYSMVS:CMS Sampled
Open Linux_AMS_Alert_Critical zmanageapmgw:LZ 03/13/18 12:23:14 03/13/18 12:23:14 ESYSMVS:CMS Pure
Open MS_Offline MVSE.WSPOT08Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT29Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT30Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT16Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT22Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT28Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT21Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT27Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT25Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT12Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT20Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT32Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT17Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT13Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT33Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT23Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT05Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT19Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
Open MS_Offline MVSE.WSPOT10Z 03/09/18 17:47:05 03/09/18 17:47:04 ESYSMVS:CMS Sampled
ICSF Subsystem Status
Status CryptoSvcs CCMKeyOK 1 CC 1 CMOS 1 PCI PCIStatus PRSM CICSWAITL DES Version ASID SSMODE DomainIdx CDMF
Active Active No No No No None No 00AAB0B0 Enabled 05.29 176 Unknown -1 Disabled
CKDS 80Full CCC CKDSAccess CKDSname WLDsname MKVer MKey
Unknown Unknown ? ? -1 ?
PKAMKeys KMMK CMOS0 KMMK CMOS1 SMK CMOS0 SMK CMOS1 PKACall PKDSRead PKDSWrite PKDSname
Invalid Unknown Unknown Unknown Unknown Unknown Unknown Unknown ?
KMMKey SMKey MonStatus AvgWait SCEDisabled
? ? Unknown 9 -1
Hub Time: Tue, 03/13/2018 07:06 PM
Server Available
Cryptographic Services -

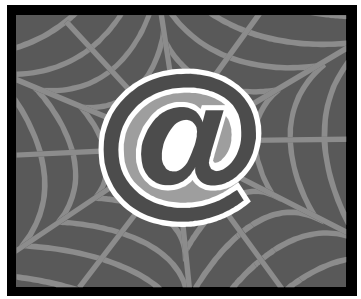
Omegamon Counters



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

- 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=swg27005524

Questions …