MAINFRAME CRYPTO

Unscrambling the Complexity of Crypto!

Transporting Crypto Keys

gregboyd@mainframecrypto.com



Copyrights and Trademarks

C) 2022

- Copyright © 2022 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.

CCA/ICSF - ICSF

© MAINFI

Page 3

CSFPlex Sharing Data Sets



February 2022

(C) MAINFE

Page 4

Also how Disaster Recovery Works



Shared Data, Unique key store, Common MK





© MAINF

Page 5

February 2022

Common master key - Copy the key

- IDCAMS REPRO
- KeyXfer Tool (GitHub)

IDCAMS REPRO

//SAVEKEYS EXEC PGM=IDCAMS,REGION=4M

//CKDSP DD DSN=PROD.CSF.CSFCKDS,DISP=SHR

//SEQP DD DSN=savekey.dsn,DISP=(,CATLG),

// SPACE=(TRK,(1,1)),UNIT=SYSALLDA,

```
// DCB=(LRECL=372,BLKSIZE=2048,RECFM=VB)
```

```
//SYSPRINT DD SYSOUT=*
```

```
//SYSIN DD *
```

```
REPRO INFILE(CKDSP) OUTFILE(SEQP) -
```

FROMKEY(key label to be copied) –

COUNT(1)

Primary PROD CKDS

Bkup key data set

IDCAMS REPRO

//RESTKEY EXEC PGM=IDCAMS,REGION=4M

//SEQT DD DSN=savekey.dsn,DISP=SHR

//CKDST DD DSN=TEST.CSF.CSFCKDS,DISP=SHR

//SYSPRINT DD SYSOUT=*

//SYSIN DD *

/*

REPRO INFILE(SEQT) OUTFILE(CKDST)

Bkup key data set Primary CKDS

KeyXfer Tool – REXX EXEC on GitHub

- KEYXFER OPER, LABEL, DSN, OPTION
 - OPER
 - WRITE_CKDS (read the key from the CKDS; write to file)
 - READ_CKDS (read from file; write to CKDS)
 - WRITE_PKDS (read the key from the PKDS; write to file)
 - READ_PKDS (read from file; write to PKDS)
 - LABEL fully qualified key label
 - DSN PS or PDS(member) to store the key for transfer
 - > 01/23/22 6:35PM BOYDG.PE.KEY.20211221 01000000400C082 ... C220FBC59BF ...
 - OPTION

February 2022

- OVERWRITE
- DEBUG

first 32 bytes of the key token last 32 bytes of the key token

© MA

Moving keys between systems



PEKEY1 – CIPHER key with KCV 83A156

🔰 A - Sh	are - <mark>[</mark> 32 x	80]														9 <u>000</u> 9		×
<u>File</u> <u>E</u> dit	Settings	<u>V</u> iew	Communic	ation <u>A</u>	ctions <u>W</u> i	ndow <u>H</u> el	lp											
1111	咱		6	8 1	_	2	-		•D=			@?	?					
PrtScrn	Сору	Paste	Send	Recv	Display	Color	Мар	Record	Stop	Play	Quit	Support	Index					
сомм	AND		> _	3	ICSF	- скр)S Ke	ey At	tribu	utes	and	Metad	lata	sc	ROLL		> CS	R
Acti	ve C	KDS	SHPL	EX.	52.CS	FCKDS	5											
Labe	1: B	OYDO	G.KEY>	KFER	AES2	56.CI	PHER	. D22	0209							С	IPHE	R
Rec	ord	stat	tus: A	Activ	ve		CA	rchi	ved.	Acti	ve,	Pre-a	activ	e, D	eact	ivat	ed)	
Sel 1 2 3 4	ect Mo De Di Di Di	an a dify lete spla spla	action one the ay var ay all ay all	n: or r reco riabi L IBI L ins	more ord le-le M var stall	field ngth iable atior	ds wi meta 2-len var	th t data gth iabl	he ne bloo metao e-ler	ew va ck wi data ngth	th t bloc meta	ag: ks	bloc	d: ks				
															M	ore:		
Key Alg Ler Key	Attr orit gth Usa	ibui hm: (bii ge:	tes):	AES - ENCI	RYPT	DECRY	Ke Ke PT A	y ty y ch NY-M	pe: eck v ODE	value	CI 83	PHER A156	E	NC-Z	ERO			
Key XPR Key	Man T-DE Nam	s XF	PRT-AB	XPR S XP	T-SYM PRT-R	SA PO	DRAND	XPR		Y NOE DOM	X-RA	W XPF	ктсра	C NO	СМРТ	AG		
Pres Pres	S EN	ITER	to pr to e>	it i	ss. to th	e pre	eviou	ıs me	nu.									
MA 0258	A		71 61 0 1			1 100 10 00	220 :	1 / 177	Deada								02/	015
0200	Februa	through	LSI.2 to sec	ure remo	te server/ho	st 129.40.39	7Exc	hange	Transr	orting	Kevs	1 57		V Z	57.0	Pa	ae 11	
Mar and a little			le and		1 de			indinge -	Tunop	or ung	1090		1	11/2		~ 34	90	10

© MAIN

Moving keys between systems

/* EXPORTER KEY FOR SENDING KEYS FROM A TO B */ ADD TYPE(EXPORTER) LENGTH(32) ALGORITHM(AES), CLEAR, LAB(BOYDG.KEYXFER.AES256.EXPORTER.ATOB.D220209)

🙀 A - Share - [32 x 80]	9 <u>6</u> 9		X
<u>File Edit Settings View Communication Actions Window Help</u>			
PrtScrn Copy Paste Send Recv Display Color Map Record Stop Play Quit Support Index			
COMMAND ===>			
Key Type ===> EXPORTER Outtype ===> (Optional) Label ===> BOYDG.KEYXFER.AES256.EXPORTER.ATOB.D220209 Group Labels ===> NO_ NO or YES			
Start ===> End ===>			
===>			
or Clear Key ===> YES NO or YES Control Vector ===> YES NO or YES Length of Key ===> 32 For DES: 8, 16 or 24 For AES: 16, 24, Key Values ===>	or 3	2	
Comment Line ===> EXPORTER key for sending keys from A to B Press ENTER to create and store control statement Press END to exit to the previous panel without saving			
		02/	015
Connected through TLS1.2 to secure remote server/host 129.40.39.239 using lu/pool TCPS219 and port 6001 February 2022 ZExchange - Transporting Kevs	Pac	ue 13	

CKDS Keys Utility View of Exporter Key

KEYOUT Data Set

BROWSE BOYDG.KGUP.KEYOUT	Line 000000000 Col 001 080 Scroll ===> CSR
+3+3+	478
••••••••••••••••••••••••••••••••••••••	of Data **********************************
Command ===>	Scroll ===> CSR
+9+0+1+- *************************	2
**************************************	tom of Data **********************************
BROWSE BOYDG.KGUP.KEYOUT	Line 0000000 Col 161 240
+	Ø+1+2+3+
**************************************	op of Data

- 64 Bytes
- 8 Bytes
- 64 Bytes

• 8 Bytes

Key Type Either the TRANSKEY label or CLEAR

Page 15

Кеу Туре

Key Label

• Variable Length Key Token

ADD LABEL(BOYDG.KEYXFER.AES256.IMPORTER.ATOB.D220209), TYPE(IMPORTER) CLEAR, ALGORITHM(AES), KEY(6DD7EB29D0F7576B, 80094FA878F4B71A, 2D35E4CEC372535E, C43A823337FC7447)

BROWSE BOYDG.KGUP.KEYOUT	Line	0000000000 Scrol	Col 141	22Ø CSR
+8+9- 	+	Ø+	-1+	2
	+	0+	-1+	2
+++++ Top of Data +++++	+++++	*********	*****	++++
_PÔ.}7ï,Ø. yÌ4¾UóCÊë;D.bÜÈå				
44446DE2DF56804A7FB123ECC755C3833F7400000000000000000000000000000000000	0000000	000000000000000000000000000000000000000	00000000	00000
***** Bortom of Data ***	******	*********	******	****

zExchange - Transporting Keys

New Key Label, New Key Type, Same KCV

zExchange - Transporting Keys

Transferring the operational key

- CSNBKEX Key Export
 - Takes a key from being encrypted under a master key to being encrypted under an exporter key-encrypting key
- CSNBKIM Key Import
 - Takes a key from being encrypted under an importer key-encrypting key to being encrypted under a master key
- CSNDSYX
 - Takes a symmetric key from being encrypted under a master key to being encrypted under an RSA public key or AES Exporter key
- CSNDSYI
 - Takes a symmetric AES or DES DATA key from being encrypted under an RSA public key to being encrypted under a master key
- CSNDSYI2
 - Takes a symmetric HMAC, AES or DES key from being encrypted under an RSA public key or an AES EXPORTER key to being encrypted under a master key

Transporting AES keys

 Multi-step process to wrap/unwrap an existing AES DATA key with AES IMPORTER/EXPORTER keys derived from an ECC Key Pair. <u>https://community.ibm.com/community/user/ibmz-and-linuxone/viewdocument/drvaesmp?CommunityKey=6593e27b-caf6-4f6c-a8a8-10b62a02509c&tab=librarydocuments</u>

• Set of REXX EXECs to

- GENECC2 Create a public/private key pair on A and export the public key to B
- GENECC2 Create a public/private key pair on B and export the public key to A
- IMPRTEC2 On A, import B's public key
- IMPRTEC2 On B, import A's public key
- DRVAESXP On A, create an EXPORTER key using A's private key and B's public key
- DRVAESMP On B, create an IMPORTER key using B's private key and A's public key
- ESPAES32 On A, export the operational key using the EXPORTER key
- IMPAES32 On B, import the operational key using the IMPORTER key

Diffie-Hellman Key Exchange

- Alice and Bob agree to use specific values for a modulus and base
 - Modulus p 23
 - Base g 5
- Alice selects a secret value ... we'll use 4 and
 - Calculates A = g^a mod p => A = 5⁴ mod 23 = 4
 - And shares A with Bob
- Bob selects a secret value ... we'll use 3 and
 - Calculates B = g^b mod p => B = 5³ mod 23 = 10
 - And shares B with Alice

February 2022

- Alice computes the shared secret s
 - s = B^a mod p => 10⁴ mod 23 = 18
- Bob computes their shared secret s
 - S = A^b mod p => 4³ mod 23 = 18

From Wikipedia: https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

Create ECC Pair for AtoB and BtoA

On A-Generate ECC Public/Private Key Pair

🔛 A -	Share -	[32 x 8	30]													8 <u>10 - 1</u> 92		×
<u>File</u>	dit Set	ttings	View	Communie	ation A	tions <u>W</u> i	ndow <u>H</u> e	lp										
-						*	۵.		•			D	-2	-				
Щ	4	8	8				È			•			⊕.	1				
PrtScrr	n Co	ру	Paste	Send	Recv	Display	Color	Мар	Record	Stop	Play	Quit	Support	Index				
								- IC	SF -	PKD	S Key	's						
E	nter		he F	KDS	recor	d's	label	for	the	act	ions	belo	~~					
	==>	BO	YDG.	KEYX	FER.A	TOB.	KEYPA	AIR.D	02202	09								
S	elec	t (one	of th	ne fo	llow	ing a	actic	ons t	hen	press	ENT	ER to	proce	255:			
	Con		-	-	BS						d 50	lost		kov ti		-		
	RSA	Ak	ey b	it le	ength	1: _	512	=y pe	1024		2048	3	072	4096	5			
	EC	NI	ST C	urve		-	p192	-	p224	_	p256	_ F	384	5 p521		94		1.2
	Ent	er	Pri	vate	Key	Name	(opt	iona	1)	_	9224		230	_ psze	, _ Þ3	84	_ p_	12
		=>	BOYD	G.KE	YYXFE	RAT	OB.KE	EYPA1	R PR	IVAT	E.D22	0205)					
	Del	let	e th	ne ex	istir	ng pu	blic	key	or k	ey p	air P	KDS	recor	d				
	Exp	or	t th	e PKI	os re	cord	'S DL	blic	kev	to	a cer	tifi	cate	data s	et			
	Ent	er	the	DSN		=>												
	Ent	ler V=	des	ired	subj	ect'	s con	mon	name	(op	tiona	1)						
				-	TIP: COMP.													
	Ent	eate cer	e a the	DSN	pub	-> K	ey re	ecord	I Tro	m an	тпри	IT CE	ertiti	icate.				
																	00	000
A256	Conne	erted +	hrough 1		ure remot	e server/ho	ct 120 40 20	230 using	lu/neel TC	D\$210 and	nort 6001						08/	003
	Febr	ruarv	2022	2012 10 50	ure remot	e server/no	31 125,40.55	ZEXCH	ange -	Transn	orting K	evs	y , 1	and the	7 ,1	Pac	1e 22	

zExchange - Transporting Keys

Page 22

On A - Export the public key

WA - Share - (32 x80) File jdit Settings View Communication Actions Window Help Image:																		
<pre>Ele Edit Settings View Communication Actions Window Help File Edit Settings View Communication Actions Window Help Prison Copy Paste Send Rev Display Color Map Record Stop Play Out Support Index Prison Copy Paste Send Rev Display Color Map Record Stop Play Out Support Index Prison Copy Paste Send Rev Display Color Map Record Stop Play Out Support Index Prison Copy Paste Send Rev Display Color Map Record Stop Play Out Support Index Prison Copy Paste Send Rev Display Color Map Record Stop Play Out Support Index Prison Copy Paste Send Rev Display Color Map Record Stop Play Out Support Index Prison Copy Paste Send Rev Display Color Map Record Stop Play Out Support Index Prison Copy Paste Send Rev Display Color Map Record Stop Play Out Support Index Prison Copy Paste Send Rev Display Color Map Record Stop Play Out Support Index Prison Copy Paste Send Rev Display Color Map Record Stop Play Out Support Index Prison Copy Paste Send Rev Display Color Map Record Stop Play Out Support Index Prison Copy Paste Send Rev Display Color Map Record Stop Play Out Support Index Prison Copy Paste Send Rev Display Color Map Record Stop Play Out Support Index Prison Copy Paste Send Rev Paste Rev Paste Prison Play Color Paste Prison Paste Rev Paste R</pre>	🔛 A	- Share - [32	x 80]													2 <u>11</u> 2		<
Image: A product of the state of the st	<u>F</u> ile	<u>Edit</u> <u>S</u> ettin	gs <u>V</u> iew	<u>C</u> ommuni	ication <u>A</u>	ctions <u>W</u> i	ndow <u>H</u>	elp										
Prison Copy Paste Send Rev Display Color Map Reord Stop Play Quit Support Index ICSF - PKDS Keys Command Select one of the abel for the actions below > BoyDG, KeyXFER, ATOB, KEYPATR, D202090 Select one of the following actions then press ENTER to process: Generate a new RSA or EC key pair record. Select one key type/size RSA key bit length: 512 1024 2048 3072 4096 EC NIST Curve p192 p224 p286 p384 p512 EC Brainpool Curve: p160 p192 p224 p286 p384 p512 ==> Delete the existing public key or key pair PKDS record stop p384 p512 ==> Delete the PKDS record's public key to a certificate data set enter the DSN ===> ==> FEYXFER XS09CERT ATOB Enter the DSN ===> FEYXFER S09CERT ATOB Enter		ቤ				-*	2			•D=			@ ?	7				
COMMAND ===> Enter the PKDS record's label for the actions below ==> BOYDG.KEYXFER.ATOB.KEYPAIR.D22099 Select one of the following actions then press ENTER to process: Generate a new RSA or EC key pair record. Select one key type/size RSA key bit length:10242048307240956 EC NIST Curve :P160P192P224P256P320P384P512 Enter Private Key Name (optional) ==> Delete the existing public key or key pair PKDS record S Export the PKDS record's public key to a certificate data set Enter desired subject's common name (optional) CN= Create a PKDS public key record from an input certificate. Enter the DSN ===> 	PrtScr	п Сору	Paste	Send	Recv	Display	Color	Мар	Record	Stop	Play	Quit	Support	Index				
<pre>Enter the DKDS record's label for the actions below =>> BOYDG.KEYXFER.ATOB.KEYPAIR.D220200 Select one of the following actions then press ENTER to process: </pre>		MMAND						I(CSF -	PKD	S Key	ys -						
Select one of the following actions then press ENTER to process: Generate a new RSA or EC key pair record. Select one key type/size RSA key bit length: _ 512 _ 1024 _ 2048 _ 3072 _ 4096 EC NIST Curve : _ p192 _ p224 _ p256 _ p384 _ p521 E Riter Private Key Name (optional) => Delete the existing public key or key pair PKDS record E Export the PKDS record's public key to a certificate data set Enter the DSN ===> <u>KEYXFER.XS09CERT.ATOB</u> Enter the DSN === <u>KEYXFER.XS09CERT.ATOB</u> Enter the DSN === <u>KEYXFER.XS09CERT.ATOB</u> Enter the DSN == <u>KEYXFER.XS09CERT.ATOB</u> Enter the DSN == <u>KEYXFER.XS09CERT.ATOB</u> Enter the DSN == <u>KEY</u>	E	nter	the	PKDS	recor	rd's	labe	l for	r the	act	ions	belo	w					
<pre>Select one of the forthold by the forthol</pre>	~		0100	OF T			ner .			hon				-				
<pre>RSA key bit length: _ 512 _ 1024 _ 2048 _ 3072 _ 4096 EC NIST Curve : _ p192 _ p224 _ p256 _ p384 _ p521 Enter Private Key Name (optional) =>> Delete the existing public key or key pair PKDS record Enter the DSN ===> <u>KEYXFER.XS09CERT.ATOB</u> Enter desired subject's common name (optional) CN= Create a PKDS public key record from an input certificate. Enter the DSN ===></pre>		Cono	to		BE		EC IN											
<pre>EC NIST Curve : _ p192 _ p224 _ p256 _ p384 _ p521 Enter Private Key Name (optional) ==> Delete the existing public key or key pair PKDS record Export the PKDS record's public key to a certificate data set Enter the DSN ===> KEYFFER.X509CERT.ATOB Enter desired subject's common name (optional) CN= Create a PKDS public key record from an input certificate. Enter the DSN ===> (Create a PKDS public key record from an input certificate. Enter the DSN ===> (Create a PKDS public key record from an input certificate. Enter the DSN ===> (Create a PKDS public key record from an input certificate. Enter the DSN ===> (Create a PKDS public key record from an input certificate. Enter the DSN ===> (Create a PKDS public key record from an input certificate. Enter the DSN ===> (Create a PKDS public key record from an input certificate. Enter the DSN ===> (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input certificate. (Create a PKDS public key record from an input cer</pre>	_	RSA	key	bit l	ength	h: _	512	ey pa	1024	ecor	2048	etec	3072	_ 409	G	ze		
<pre>Enter Private Key Name (optional) ==> Delete the existing public key or key pair PKDS record Export the PKDS record's public key to a certificate data set Enter the DSN ===> <u>KEYXFER.XS09CERT.AT08</u> Enter desired subject's common name (optional) CN= Create a PKDS public key record from an input certificate. Enter the DSN ===> HAT A</pre>		EC N	IST	Curve	CHEVE		p19	2 _	p224		p256	_ !	384	_ p52	1	284	051	7
 Delete the existing public key or key pair PKDS record Export the PKDS record's public key to a certificate data set Enter the DSN ===> KEYXFER.XS09CERT.AT0B Enter desired subject's common name (optional) CN= Create a PKDS public key record from an input certificate. Enter the DSN ===> 		Ente	r Pr	ivate	Key	Name	(op	tion	al)		PZZŦ	_	230	_ pbz	_ p.	504	_ por	
<pre>S Export the PKDS record's public key to a certificate data set Enter the DSN ===> KEYXFER.X509CERT.ATOB Enter desired subject's common name (optional) CN=</pre>	_	Dele	te t	he ex	istir	ng pu	blic	key	or k	ey p	pair f	PKDS	reco	rd				
Enter desired subject's common name (optional) CN= Create a PKDS public key record from an input certificate. Enter the DSN ===> 18/02	S	Expo Ente	rt t r th	he PK e DSN	DS re	=> <u>K</u> E	YXFE	R.X5	c key 09CER	T.AT	OB	rtif	icate	data	set			
Create a PKDS public key record from an input certificate. Enter the DSN ===>		Ente CN=	r de	sired	sub	ject'	s co	mmon	name	(op	otiona	al)						
Enter the DSN ===>	_	Crea	te a	PKDS	publ	lic k	ey r	ecord	d fro	m ar	n inpu	ut ce	ertif	icate.				
		Ente	r th	e DSN		=>												
	MA	A															18/0	25

Connected through TLS1.2 to secure remote server/host 129.40.39.239 using lu/pool TCPS219 and port 6001

256

On A – PKDS Keys Utility

Import A's Public Key on B

On B - Import the Public key from A

February 2022

鯞 B - WS	CLAB1 - [3	32 x 80]															<u></u> ?		×
<u>File</u> <u>E</u> dit	Settings	View	Communi	ication <u>A</u>	Actions <u>W</u> i	ndow <u>H</u> e	elp												
	Ð			8 1	đ		-		•D=			●?	?						
PrtScrn	Сору	Paste	Send	Recv	Display	Color	Мар	Record	Stop	Play	Quit	Support	Index						
СОММ	IAND		=> _		- ICS	F –	PKDS	Key	Att	ribu	tes	and	Meta	adata	sc	ROLL	>	PA	AGE
Acti	vel	PKD	5: LA	BPLE	EX.PK	DSR.	NEW												
Labe	1: I	BOYI	DG.KE	YXFE	R.AT	OB.A	PUBL	IC.D	2202	09									
Rec	ord	sta	atus:	Act	tive			CAre	⊂hiv	ed,	Acti	ve,	Pre	-activ	e, D	eacti	vate	(b	
Sel	ect M	an odi ele	acti fy on te th	on: le or le re	mor	e fi	elds	witl	n th	e ne	w va	lues	spe	ecifie	d				
Pres Pres	S E		to	proc exit	t to	the	prev	ious	men	ч.									
																Me	re:		
Key	Att	rib	utes																
Alg	ori	thm	: E	CC				Curr	ve:			PRI	ME						
P (bit	5)	5	21				QC	byte	s):		133							
Sec	tio	ns:	P	UBLI	C														
Pul		N=	Y																
	040 589 BDC CCC F15	164 3D7 BC50 17FI D404	1814F 7DBE6 00567 =A262 4ABE	D767 F1F9 D249 3004	7284C 58441 94308 4F79D	8671 E51E 0501 C319	7119 74AA D785 030E	57BC 59DC 7BE60 7DC80	914D BAED C433 DE32	FØ2D C69F 3ØB7 C4BB	3213 B45C 4661 2869	86CB 6D11 .B400 33B9	818: AEB4 Ø1C4 E4AB	116D39 4A936A 401209 BE6BBD	384D 6EF1 AC16 3484	741B ADA2 E58D EE53			
M A	В																	02/0	015
1200 Se	cure sock	et is con	necting thro	ough to re	emote server	/host lab1.	.wsclab.wa	shington.ib	m.com us	ing port 99	2								

zExchange - Transporting Keys

Page 28

Repeat for B to A

- Generate a public/private key pair on B
- Export the public key from B to a file
- Move that certificate file to A
- Import the public key from B, on A

C MAINE

Page 30

Create AES Exporter on A

On A – Execute DRVAESXP REXX to Create the Exporter key

🔛 A - S	hare - [32 :	x 80]														9 <u>00</u> 9		×
<u>F</u> ile <u>E</u> d	it <u>S</u> etting	s <u>V</u> iew	Communi	cation <u>A</u>	ctions <u>W</u>	indow <u>H</u>	elp											
	G			.	-*	2			•D=			@ ?	7					
PrtScrn	Сору	Paste	Send	Recv	Display	Color	Мар	Record	Stop	Play	Quit	Support	Index					
M	enu	Uti	litie	s <u>C</u>	ompil	ers	Help	Þ	1.00			T MAX						
BRO	WSE mand	s ===	YS220	40.T	20555	4.RA	000.1	BOYDG	.RØ1	00635	5	Line	000	00000	00 Coroll	ol Ø ====	01 > <u>C</u>	080 SR
EXEC	'BO	YDG.	TOOLS	REX	×. EXE	C(DR	VAES	TOP O XP)'	f Da	ta *		* * * * *	+ + + +	* * * * *	++++	* * * *	+++	* * * *
deri 209	ved /	AES	EXPOR	TER	key l	abel	: 80	YDG.K	EYXF	ER.A	ES256	5.EXP	ORTE	R.FRO	MECC	ATO	B.D	220
End	of Sa	ampl	 e															
	****		*****	* * * *	*****	++++	++ Bo	ottom	of	Data	+++	* * * * *	* * * *	* * * * *	* * * *		***	* * * *
MA	A		_														04	/015
0200	Connected	through	ILS1.2 to se	cure remo	te server/ho	ost 129.40.3	9.239 usin	g lu/pool T	.PS219 an	d port 6001	IZ - III		-			-	04	,ti

0

On A – Exporter key KCV=935392

🔛 A - Sh	are - [32 x	80]														9 <u>6.</u>		×
<u>File</u> <u>E</u> dit	Setting	s <u>V</u> iew	Communic	cation A	ctions <u>W</u> i	ndow <u>H</u> e	lp											
PrtScrn	Сору	Paste	Send	Recv	Display	Color	Map	Record	•D= Stop	Play	Quit	() Support	? Index					
COMM	AND ve 0	====	> _ : SHPI	LEX.	ICSF S2.CS	- CKI	DS Ke	≥y At	trib	utes	and	Metad	lata	 S	CROL	.L ==	==> C	SR
Labe	1: E	OYDO	G.KEY)	XFER	AES2	56.E>	KPORT	FER.F	ROME	CC.AT	ОΒ.С	22020	99				EXPO	RTER
Rec	ord	stat	tus: /	Acti	ve		CA	Archi	ved,	Acti	ve,	Pre-a	activ	/e,	Deac	tiva	ated)	8
Sel 2 2 2	ect Mo De Di Di Di	an a dify lete spla spla	action y one e the ay van ay al ay al	n: rec riab l IBI l in:	more ord le-le M var stall	field ngth iable atior	ds wi meta e-ler n var	ith t adata ngth riabl	he n blo meta e-le	ew va ck wi data ngth	th t bloc meta	ag: ks data	bloc	ed :ks				
																More	e :	-
Key Ala Ler Key WR-	Attr orit gth Usa AES	ibut hm: (bit ge: WR-H	tes ts): HMAC N	AES - EXP WR-D	ORT T ATA W	RANSI R-KEP	Ke LAT C K WR-	≧y ty ≧y ch GEN-O -PIN	pe: eck PEX WRDE	Value GEN-I RIVE	EX 93 N EX WR - C	CEN CEN		GEN	ZERO - PUB	WR	-DES	
Key Key	Mar T-AE Nar	s XI	nent: PRT-R	XPR SA P	T-SYM OKEYA	XPRI GR P(TUASY	Y XPR Agr	TAAS	Y NOE	X-RA	W NOC	⊆МРТ≠	AG X	PRT-	DES		
Pres	S EN	ITER	to pi to e	roce	ss. to th	e pre	≥viou	us me	nu.									
MA	A																02	/015
<mark>@256</mark>	onnected	through	TLS1.2 to see	cure remo	te server/ho	st 129.40.39	9.239 using	g lu/pool TC	PS219 an	d port 6001			-		-	-		di
NL.	i ebrua	ary 202	The state	-11		-	ZEXC	nange -	rans	porting	neys	14		N/-	1		Page 32	11

© MAIN

Create AES Importer on B

On B – Importer key KCV=935392

February 2022

🐱 B - WSCLAB1 - [32 x 80]				- 🗆 X
File Edit Settinger View Communication Actions Window Hole				
rie Edit Settings view Communication Actions window riep				
		· □ ? '	2	
			•	
PrtScrn Copy Paste Send Recv Display Color Map	Record Stop Play	Quit Support In	dex	
ICSF - CKDS	Key Attrib	utes and Me	tadata	
COMMAND ===>			SCROLL :	===> PAGE
Active CKDS: LABPLEX.CKDSR.NEW				
Label BOYDG KEYXEER AES256 TMP	ORTER EROME	CC ATOB D22	0209	TMPORTER
Label: Borbo.RETATER.AE5250.111		CC. A 08.822	0203	111 OKTER
Record status: Active	(Archived,	Active, Pr	e-active, Deactive	vated)
Select an action:				
2 Delete the record	with the h	ew values s	pectried	
			Mo	re: +
Metadata	YYYYMMDD		YYYYMMDD	
Record creation date:	20220209			
Cryptoperiod start date:	000000000	New valu		
Cryptoperiod end date:	000000000	New valu	ie:	
Date the record was last used:	20220210	New valu	le:	
Service called when last used:				
Date the record was recalled:	00000000			
Date the record was archived:		New yerley	10.	
Prohibit archive flag:	FALSE	New valu		
Key Attributes				
Algorithm: AES	Key type:	IMPO	DRTER	
Length (bits): -	Key check	Value: 9353	92 ENC-ZERO	B DES
WR-AES WR-HMAC WR-DATA WR-KEK	WR-PIN WRDE	RIVE WR-CAR	D	R-DES
MA B				02/015
9256 Connected through Telnet-negotiated security TI \$1.2 to secure remote serv	er/host lab1.wsclab.washingt	on.ibm.com using lu/pool L	AB10462 and port 9	
we w	en nos las invacionas inige	entirent and a poor of		222

zExchange - Transporting Keys

Page 34

A: Export PEKey1 & B: Import PEKey1

0

On A – Export the CIPHER key

🔰 A - Sh	nare - <mark>[</mark> 32 x	80]														9 <u>1 - 1</u> 9		X
<u>File</u> <u>E</u> dit	<u>Settings</u>	<u>V</u> iew	Communi	ication A	ctions <u>W</u> in	dow <u>H</u> elp												
	G			.		2			•D=			@ ?	7					
PrtScrn	Сору	Paste	Send	Recv	Display	Color	Мар	Record	Stop	Play	Quit	Support	Index					
Me	enu	Util	litie	s <u>C</u>	ompil∈	ers .	Help		0	070/		15.0						
BROV	VSE	รา	rs220	40.T	212800	. RAØ	ØØ.В	OYDG	.RØ1	00637	7	Line	0000	00000	00	Col	001	080
Comn	nand	++++	- + + + + +	* * * *	*****		++ T	op o	f Da	ta **	* * * * *	*****		Sc +++++	rol +++	1 ===	=> <u>C</u>	<u>SR</u> + + + +
EXEC	BOY	DG.T	TOOLS	REX	X.EXEC	EXP	AES3	2)'			- 00	200000	0.0					
verif	ficat	ion	patt	ern:	8FF11	L79E7	891E	672	-n cri		- 00		. 00					
expor 02000	00880	5000		202E	F3BE3E	8881	CEA5	A000	0000	00000	00000	002020	00000	0100				
001A0	00000	0000 EE13	02800 2808	0020 E75E	001020	000F	F000	3E80	0000	00214	4A5C	DA4E43	63CF					
06486	31A2F	58B1	1687A	9886	8F3741	9706	7A7F	3A4D	CA54	D9A3F	C3D/	AC53B8	33828	3851				
expor	ted	key	LENG	тн:	136													
expor	ted	key	leng	th (hex):	000	0008	8×										
End o	of Sa	mple	≥															
++++	* * * * *	++++	* * * * *	* * * *	* * * * * *	****	* Bo	ttom	of	Data	++++	*****	****	*****	+ + +	* * * *	* * * *	* * * *
														PEK	KEY	1		
													K	C = 8	33 A	156		
MA	A																04	/015
	Ealer	om 00		~			-	<u></u>						<u> </u>		<u></u>	1	9:28 PM
N. N	repru	ary 202	11	11	- Ve	1	ZEXC	hange	- Trans	porting	Keys	5 11	C a	V. N	1		age 36	7

On B – Import the CIPHER key

February 2022

Eile Edit Settings View Communication Actions Window Help Image: Settings View Communication Actions Window Help Prise: Composition Copy Paste Send Recv Display Color Map Record Stop Play Quit Support Index EDIT BoyDg. Tools. REXX. EXEC (IMPAES32) - Ø1.Ø2 Columns ØØØØ1 ØØØ72 Scroll ===> CSR ØØØØ24 /* - Execute this script from TSO */ ØØØØ25 /* (e.g. EX 'HLQ.MLD.LLQ(IMPAES32)') Ø1.Ø2 Columns ØØØØ1 ØØØ72 ØØØØ26 /* (e.g. EX 'HLQ.MLD.LLQ(IMPAES32)') */ ØØØØ26 /* (e.g. EX 'HLQ.MLD.LLQ(IMPAES32)') */ ØØØØ28 /* Pre-existing key labels in use for this sample */
Image: Note of the state o
FileEditEdit_SettingsMenuUtilitiesCompilersTestHelpEDITBOYDG.TOOLS.REXX.EXEC(IMPAES32) - 01.02Columns0000100072Command ===>Scroll ===>Scroll ===>CSR000024 /* - Execute this script from TSO+/000025 /*(e.g. EX 'HLQ.MLD.LLQ(IMPAES32)')+/000026 /*
EDIT BOYDG.TOOLS.REXX.EXEC(IMPAES32) - 01.02 Command ===> 000024 /+ - Execute this script from TSO 000025 /+ (e.g. EX 'HLQ.MLD.LLQ(IMPAES32)') 000026 /+
<pre>000031 LEFT('BOYDG.KEYXFER.AES256.IMPORTER.FROMECC.ATOB.D220209'.64) : 000032 000033 /* Define the key label for the received AES CIPHER key */ 000034 aes_data_key_label = LEFT('BOYDG.KEYXFER.AES256.CIPHER.D220209'.64) : 000035 000036 /* Specify data from the sender */ 000037 /* These next three variables are copied/pasted from the */</pre>
000038 /* output of the EXPAES32 REXX EXEC that was executed */ 000039 /* on the source system */ 000040 verification_pattern = 8FF1179E7891E672'×
000041 ebcrypted_Fey_= 000042 '0200008805000000202EF3BE3B88881CEA5A00000000000000000202000000100'× . 000043 '001A000000002800002000102C000FF0003E80000000214A5CDA4E4363CF0C7'× . 000044 'DA10F1228FF12BC88E75E66206A3B1C770AFDD07F556D32E8C918C0EEA93FAF1'× . 000045 '0648B1A2F58B1687A98B68F374197067A7F3A4DCA54D9A3FC3DAC53B83B28B51'× .
000047 encrypted_key_length = '00000088'x 000048 000049 /* CLEANUP the AES key label in use for this sample */ 000050 krd_label = aes_data_key_label 000051 CALL CSNBKRD
M A B 29/009 B 29/009 Connected through Telnet-negotiated security TLS1.2 to secure remote server/host lab1.wsclab.washington.ibm.com using lu/pool LAB10462 and port 9 29/009

zExchange - Transporting Keys

Page 37

A: Export PEKey1 & B: Import PEKey1

February 2022

zExchange - Transporting Keys

Page 39

Summary

- With common master keys, process is simpler, but you may have to bypass some of the security protocols
- Establishing the EXPORTER/IMPORTER keys between two systems does not have to be done every time you need to transfer keys
- There are now tools (CKDS/PKDS Keys Utility) to validate the process
- My goal here was not to intimidate ...
 - Key Management is important

References

- TechDoc Transporting AES encrypted data keys from one z/OS host to another by Philippe Richard
 - <u>https://www.ibm.com/support/pages/system/files/inline-files/Transporting_AES_DATA_keys_new.pdf</u>
- IBM Community Transporting AES Keys
 - <u>https://community.ibm.com/community/user/ibmz-and-linuxone/viewdocument/drvaesmp?CommunityKey=6593e27b-caf6-4f6c-a8a8-10b62a02509c&tab=librarydocuments</u>
- GitHub KeyXfer
 - <u>http://ftpmirror.your.org/pub/misc/ftp.software.ibm.com/s390/</u> zos/tools/keyxfer/

Questions

Page 42