z/VSE Live Virtual Class Series

Securing Data Transfers using IPv6/VSE

Jeffrey Barnard, Barnard Software, Inc.
Joerg Schmidbauer, IBM

http://www.ibm.com/zVSE
http://twitter.com/IBMzVSE

Sept, 2012

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States, other countries, or both.

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:
Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- **Basic threats (Jeff Barnard)**
- **OpenSSL on z/VSE (Joerg Schmidbauer)**
- **IPv6/VSE (Jeff Barnard)**

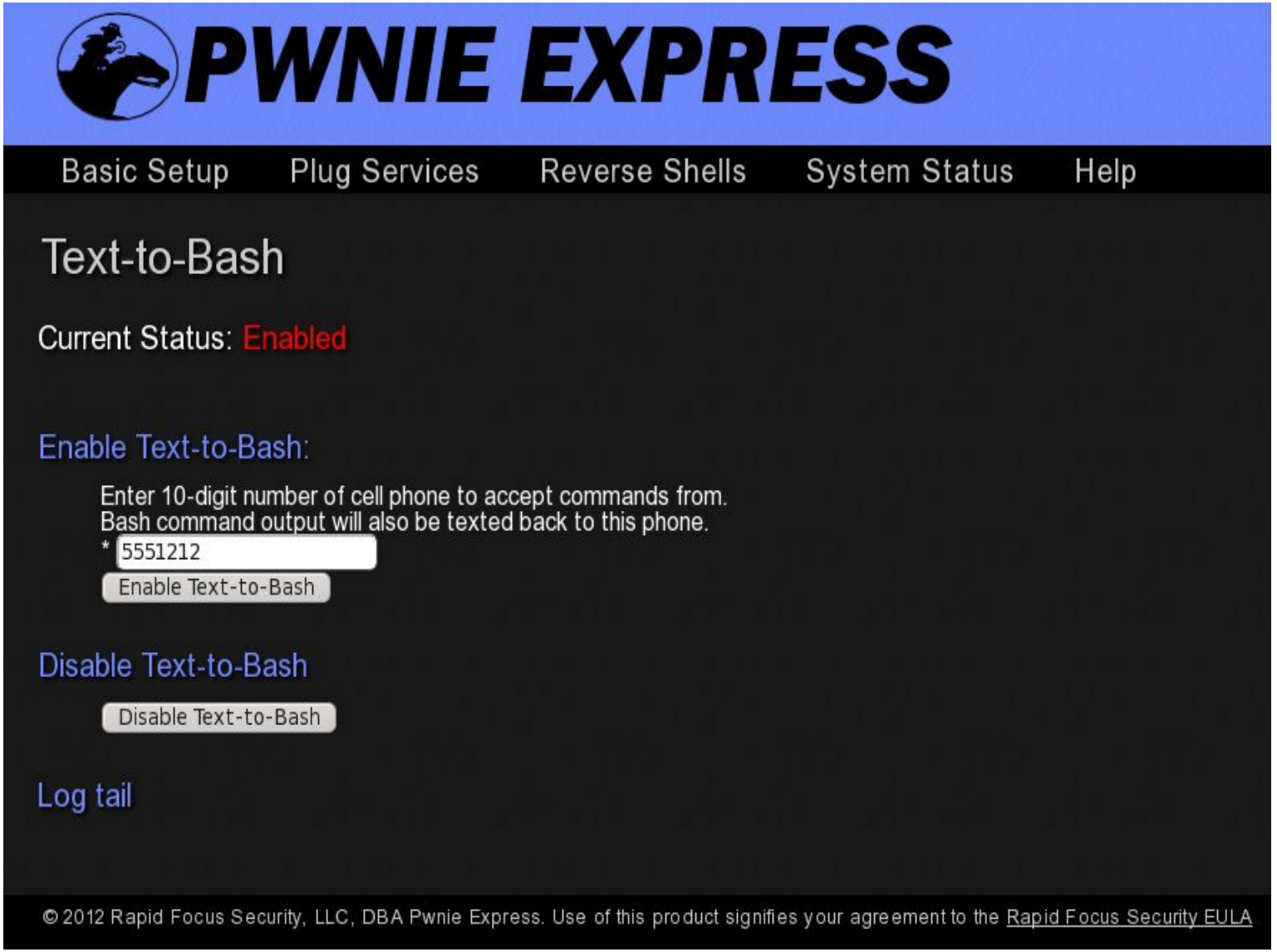
Basic threats

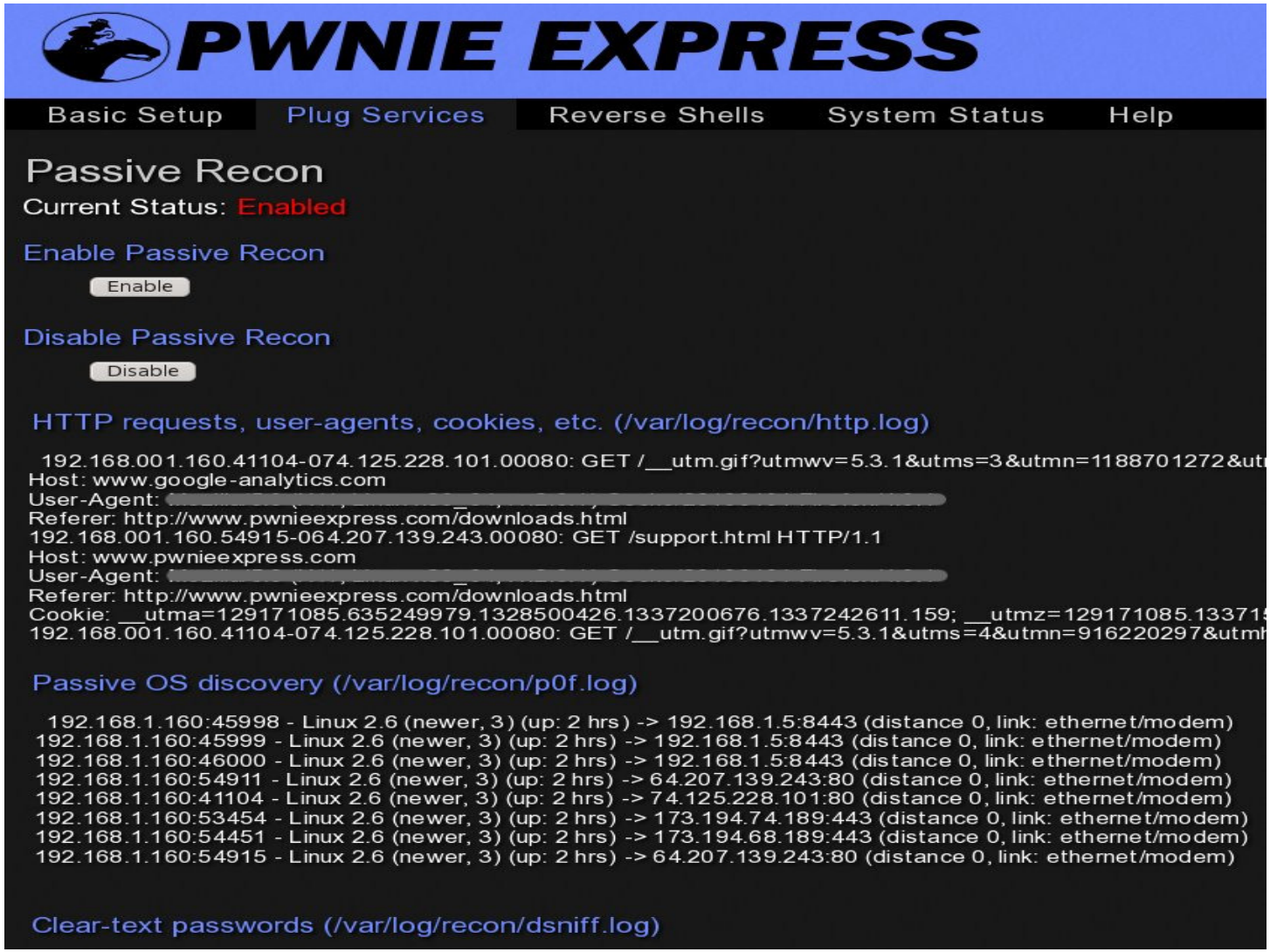
Jeff Barnard, Barnard Software, Inc.

http://www.ibm.com/zVSE
http://twitter.com/IBMzVSE

Testing platform

- **Fully-integrated enterprise-class penetration testing platform (Linux)**
- **Onboard high-gain 802.11b/g/n wireless**
- **Onboard high-gain Bluetooth (1000')**
- **Onboard dual-Ethernet**
- **Includes external 3G/GSM adapter**
- **Includes 16GB internal disk storage**
- **Fully functional 120/240v AC outlets!**





z/VSE Live Virtual Class Series

OpenSSL support in z/VSE

Joerg Schmidbauer, IBM

http://www.ibm.com/zVSE
http://twitter.com/IBMzVSE

Sept, 2012

Agenda

- **What is OpenSSL**
- **Why OpenSSL on z/VSE?**
- **What has been ported / added?**
- **RSA keys / key stores**
- **Random numbers**
- **Performance**
- **Outlook**

What is OpenSSL

- **OpenSSL is an Open Source project providing an SSL implementation and key management utilities.**
- **OpenSSL is written in C**
- **Available for most Unix-style operating systems, MAC, Windows, and:**
  IBM System i (OS/400)
- **For details on OpenSSL refer to**

  http://www.openssl.org/

Why OpenSSL on z/VSE?

- **The TCP/IP stack from Connectivity Systems, Inc. has an own SSL implementation, but:**
  - What about the other two stacks: IPv6/VSE from Barnard Systems, Inc. and Linux Fast Path (LFP) provided by IBM.
- **All stacks could use one single SSL implementation: OpenSSL**
- **OpenSSL is widely used in the industry**
- **Latest RFC's implemented**
- **One central place for access to crypto hardware, software updates, migration to higher versions**

What has been ported to z/VSE?

- **OpenSSL 1.0.0d runtime library**
  - Phase IJBSSL in PRD1.BASE
  - About 550+ C source parts and 90+ H-files
  - Total of 70.000+ Lines of code
  - Software implementations for all algorithms with all key lengths
  - Subset of the OpenSSL API
- **Built-in tests**
  - Known-answer tests for algorithms (IBM internal)
  - OpenSSL speed test (available to customers/vendors)

What has been added for z/VSE?

- **OS390 / z/OS compatible SSL API**
  - Described in “z/OS Cryptographic Services, SSL Programming”, SC24-5901
  - Consists of gsk_initialize(), gsk_secure_soc_init(), etc.
  - Allows existing z/VSE SSL applications to run unchanged
- **Hardware crypto support**
  - Crypto cards (crypto express adapters)
    - RSA encrypt/decrypt
    - RSA key generation on coprocessor cards
    - Random number generation on coprocessor cards
  - CPACF (on board crypto feature)
    - AES, TDES encrypt/decrypt
    - SHA hashing
    - PRNG (pseudo random number gen)

Two APIs available

- **GSK API**
  - Existing VSE SSL applications use the OS/390 SSL API (gsk-API), described in “z/OS Cryptographic Services, SSL Programming, SC24-5901”.
    - gsk_initialize()
    - gsk_secure_soc_init()
    - gsk_read()
    - gsk_write()
    - etc.
- **OpenSSL API**
  - The OpenSSL API consists of 200+ functions
  - A subset is available to VSE applications via IJBSLVSE.OBJ

With both APIs HW-crypto is supported.

z/VSE-specific parameters

- **GSK API: parms specified in JCL**
  - Values evaluated in gsk_initialize()
  - HW crypto support
    - `// SETPARM SSL$ICA = [ 'YES' | 'NO' ]`
  - Debug trace
    - `// SETPARM SSL$DBG = [ 'YES' | 'NO' ]`
- **OpenSSL API: parms specified via PARM='…'**
  - Values evaluated by application
  - HW crypto support:
    - Use special API functions ssl_enable_ibmca / ssl_disable_ibmca
  - Debug trace
    - Use ssl_enable_debug / ssl_disable_debug

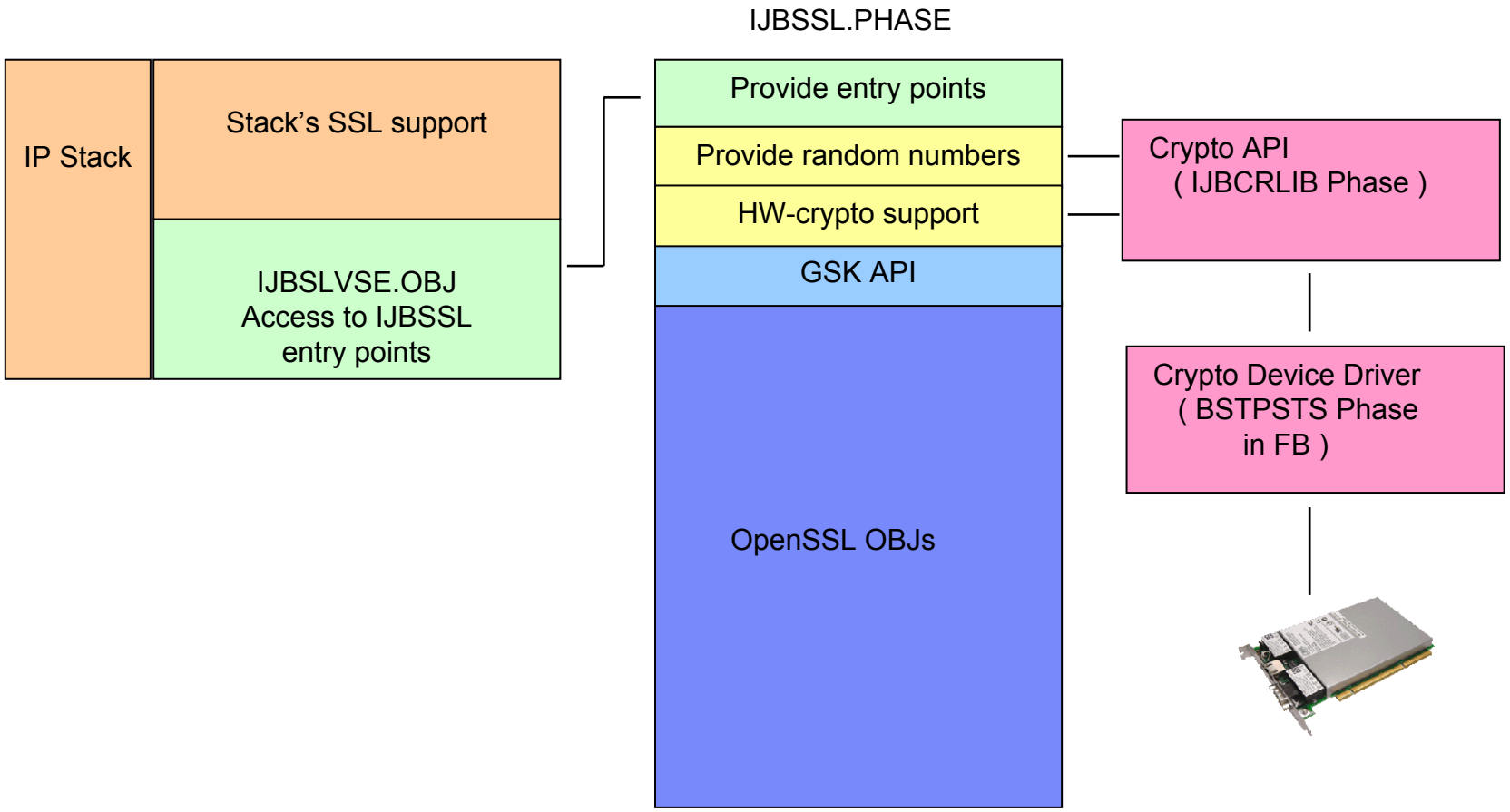
How is OpenSSL shipped on z/VSE?

- **New z/VSE 5.1 system component:**
  - z/VSE cryptographic services, 5686-CF9-17-51S
  - Installed in PRD1.BASE
  - Consists of
    - IJBSSL phase (the OpenSSL runtime)
    - SPEEDTST phase (invokes the built-in speed test)
    - NOTICES.Z (license)
    - IJBSLVSE.OBJ (provides access to the APIs)
    - IJBSSL.H (provides function prototypes)
- **Two PTFs necessary for z/VSE 5.1:**
  - DY47397 / UD53864 – OpenSSL 1.0.0d update
  - DY47414 / UD53863 – VSE/AF update for HW crypto support

What is not available on z/VSE?

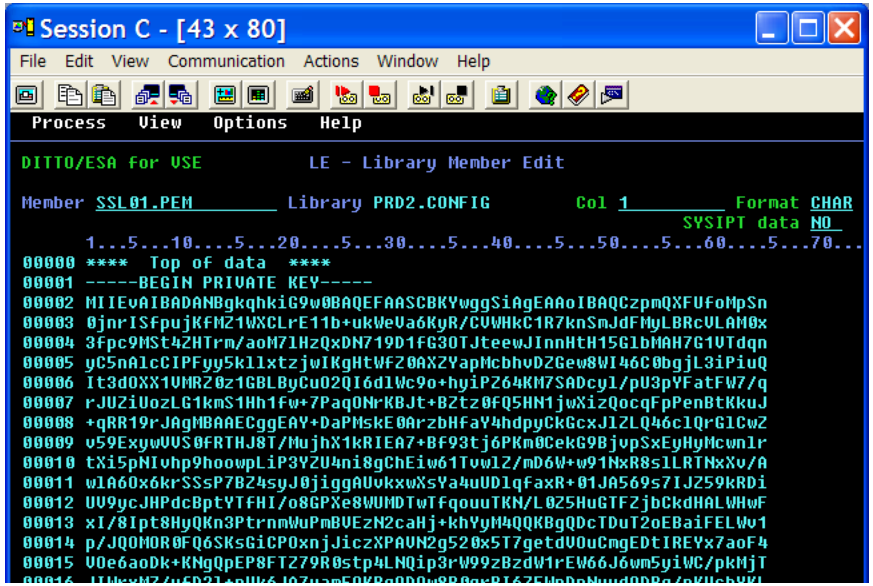
- **The openssl command line tool is not available on z/VSE**
  - Key management is done on a workstation (Windows, Linux, etc.)
  - Keystores (PEM files) are uploaded to z/VSE
- **Some algorithms are not available on z/VSE due to legal reasons**
  - IDEA, RC5, MDC2
- **Non-LE/C applications not supported**
  - OpenSSL is coded in C, therefore an LE/C-runtime environment is required for callers

How is OpenSSL integrated in z/VSE?



How do I setup my key store?

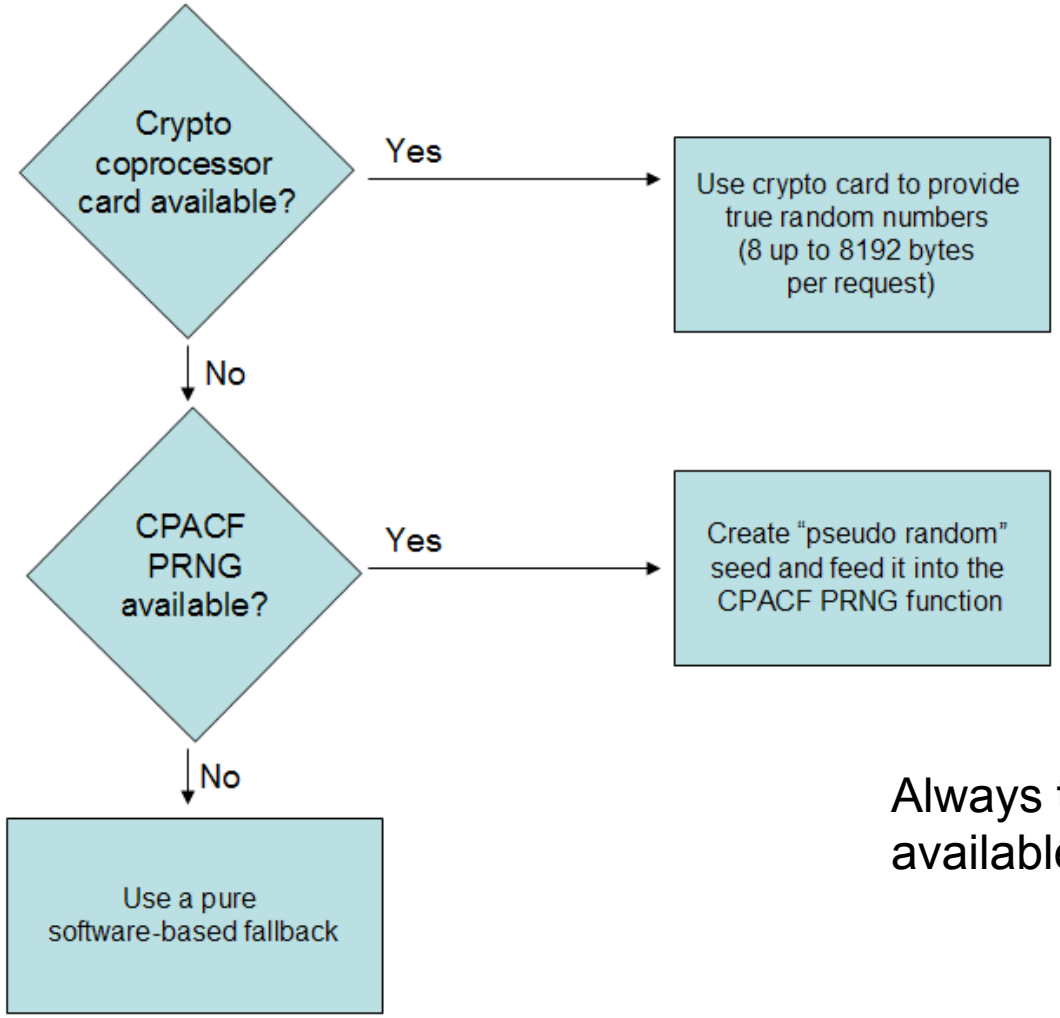
- **Step 1: create RSA key and certificate request using OpenSSL on a workstation**
  - openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout mykey.pem -out mycert.pem
- **Step 2: Sign certificate request via official CA or Keyman/VSE**
- **Step 3: Add CA certificate and VSE certificate to PEM file**
- **Step 4: When using Windows, edit the PEM file with Wordpad and save without changes.**
  - This adds the correct CRLF line endings
- **Step 5: Upload key store to VSE**
  - It's a text file, therefore use ASCII to EBCDIC translation
  - As VSE Librarian member, or
  - As VSAM file



Creating random numbers

- **Essential for the security / vulnerability of a crypto system**
- **Problem with software-based random number generators:**
  - They need a seed value (initial start value)
  - Difficulty to find good seed values:
    - TOD clock
    - Process states
    - Other sources of randomness in the system
- **Two general types distinguished:**
  - Pseudo random number generator (PRNG, software based)
  - True random number generator (TRNG, hardware based)

Random number generator on z/VSE



Always try to use best available generator

Performance

- **Built-in speed test shows performance numbers about crypto algorithms**
- **Significant performance boost with crypto hardware**
- **Invocation via SPEEDTST phase:**

```
// EXEC SPEEDTST,PARM='RSA AES-128-CBC IBMCA'

// EXEC SPEEDTST,PARM='SHA1'

// EXEC SPEEDTST,PARM='DES-EDE3 SHA256 AES-128-CBC'
```

PARM='IBMCA' enables HW-crypto for speed test

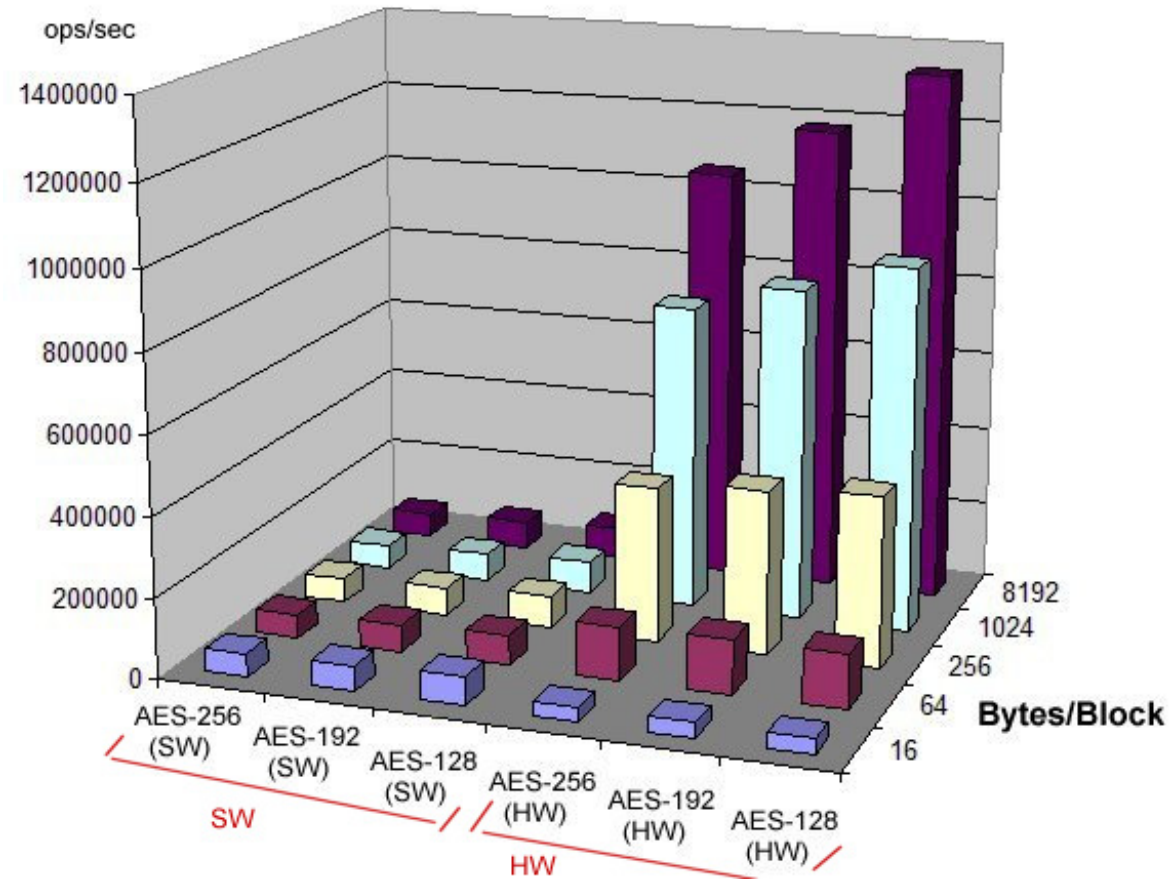
Use openssl on a workstation to get a list of possible parms:

```
openssl speed ?
```

AES Performance

Key length	Times faster with HW
AES-128	**16**
AES-192	**16**
AES-256	**17**

SW is faster for very small blocks of data due to overhead calling CPACF

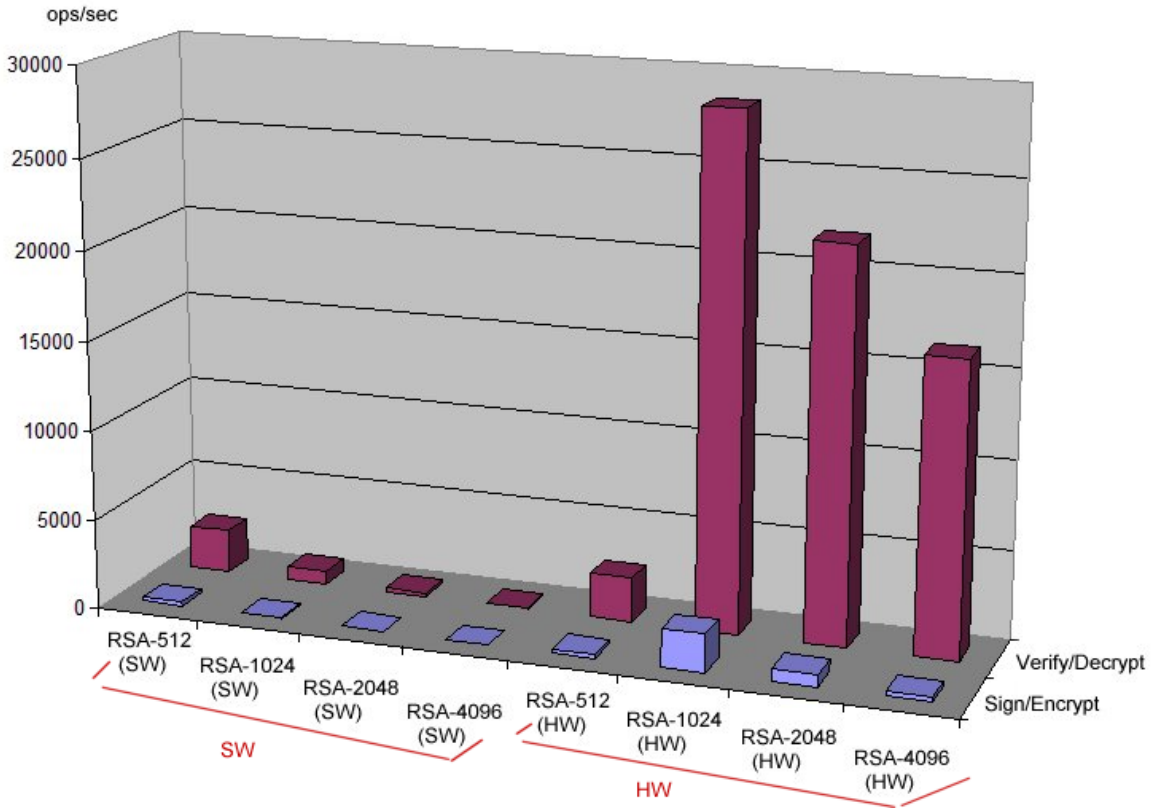


Measured on a z196

RSA Performance

Key length	Times faster with HW
RSA-512	- (*)
RSA-1024	40 - 60
RSA-2048	112 - 122
RSA-4096	302 - 308

(*) RSA-512 is not supported by HW



Measured on a z196 with Crypto Express3

Where do I find documentation?

- **Jeff Barnard's doc:**
  - IP-IPv6_VSE-SSL_Creating and Using SSL Certificates.pdf
- **IBM doc:**
  - Will be provided with next books update / release
  - White papers on z/VSE homepage (tbd): http://www.ibm.com/systems/z/os/zvse/documentation/security.html#howto

What comes next?

- **Support for non-LE apps / Assembler sockets (EZASOKET/EZASMI)**
- **Regular upgrades to latest OpenSSL service level**
- **Dynamic access to OpenSSL from all applications based on SYSID**
- **Support for DSA keys**
- **Support for Elliptic Curve Cryptography (ECC)**

More information

OpenSSL website

http://www.openssl.org/

OpenSSL License

http://www.openssl.org/source/license.html

OpenSSL command line documentation

http://www.openssl.org/docs/apps/openssl.html

A good collection of OpenSSL commands is provided at

http://www.madboa.com/geek/openssl/

z/OS Cryptographic Services, SSL Programming, SC24-5901-08

http://www.ibm.com/support/docview.wss?uid=pub1sc24590107

z/VSE Live Virtual Class Series

IPv6/VSE SSL Support

Jeff Barnard, Barnard Software, Inc.

http://www.ibm.com/zVSE
http://twitter.com/IBMzVSE

Sept, 2012

IPv6/VSE SSL support

- **Available in GA Build 252**
- **GSK API provided**
- **EZASMI, EZASOKET, LE/C support**
- **BSTTPRXY SSL Proxy Server**
- **BSTTATLS Automatic TLS Facility**

IPv6/VSE SSL Support

- **Based on IJBSSL from IBM**
- **Port of OpenSSL 1.0.0**
- **IJBSSL introduced with z/VSE 5.1**
- **C/VSE application**
- **Will run on any version of z/VSE**
- **Provides software SSL**
- **Supports CPACF and Crypto Express on z/VSE 5.1+**

IPv6/VSE SSL Support

- **IJBSSL API currently uses LE/C**
- **Requires application be LE**
- **Only batch LE applications can use GSK() API at this time. CICS not supported.**
- **These restrictions will be removed**
- **All applications are supported by the BSTTPRXY SSL Proxy Server and BSTTATLS Automatic TLS Facility**

Why convert your applications to use SSL/TLS when we will do it for you!

Proxy Types

Source	Destination
Accept clear text connection	Proxy to clear text connection
Accept SSL connection	Proxy to SSL connection
Accept clear text connection	Proxy to SSL connection
Accept SSL connection	Proxy to clear text connection
Accept IPv4 or IPv6 connection	Proxy to IPv4 or IPv6 connection

Proxy Examples

Accept a clear text connection from BSTTMTPC on port 25 and proxy the connection to an SMTP server listening on SSL port 465. This type of connection is commonly called ***smtps***.

Accept an SSL connection on port 443 and proxy the connection to CICS TS Web Services on clear text port 80. This type of connections commonly called ***https***.

Accept an SSL connection on port 992 and proxy the connection to the BSTTVNET TN3270E server on clear text port 23. This type of connection is commonly called ***telnets***.

Accept a clear text connection from BSTTFTPC on port 21 and proxy the connection to an FTP server listening on SSL port 990. This type of connection is commonly called ***ftps***.

Accept an SSL connection on port 990 and proxy the connection to the BSTTFTPS FTP server on clear text port 21. This type of connection is commonly called ***ftps***.

```
// OPTION SYSPARM='66'
// SETPARM IPTRACE='NNNNNNN'
// LIBDEF *,SEARCH=(ssllib.slib,bsilib.slib)
// EXEC BSTTPRXY,SIZE=BSTTPRXY
ID 66
*
KEYRING PRD2.CONFIG
DNAME MYCERT
SECTYPE TLSV1
*
OPTION SERVER
*
PROXY TCP V4 1234 SSL * TO V4 23 TXT * LOCALHOST
/*
```

Command	Description
ID nn	Stack ID
BUFFERSIZEK	Buffer size in K bytes The default is 16K. This is recommended.
KEYRING	KEYRING location Either VSAM -or- lib.slib
KEYFILE	Default RSA key and certificate location Either VSAM ESDS dlbl name -or library member name (member type is PEM)
SECTYPE	Security type Either SSL30 or TLSV1 TLSV1 is recommended
SESSION_TIMEOUT	Session Timeout value in seconds The default is 900.
HANDSHAKE_CLIENT	0, 3 The default is 3.
HANDSHAKE_SERVER	1, 2 The default is 1.

OPTION	FTP Indicates FTP PORT/PASV/EPRT/EPSV processing required
OPTION	SERVER|CLIENT Indicates server mode (default) or client mode
CA_AUTH	YES|NO NO is the default
CA_AUTH_TYPE	Authorization type value 0, 1, 2, 3. The default is 3. This parameter is only used when CA_AUTH is YES. 0 Validate client certificate using just the local database 1 Obtain CA certificates and certificate revocation lists not found in the local database from LDAP server 2 Obtain CA certificates and certificate revocation lists not found in the local database from LDAP server 3 Do not validate client certificate

Command	Description
PROXY	PROXY command
Protocol	TCP
IP	V4 or V6
Port	Port number
Mode	TXT (clear) or SSL (encrypted)
DNAME	DNAME member name or *
TO	
Protocol	TCP
IP	V4 or V6
Port	Port number
Mode	TXT (clear) or SSL (encrypted)
DNAME	DNAME member name or *
IP Address	IPv4 or IPv6 IP address

Handshake	Description
GSK_AS_CLIENT: (0)	Client receives server's public key and cert. Client authenticates server's public key and cert. Client checks its local CA-cert file to authenticate. DNAME = Dummy RSA key and CA-cert for authentication *(1)
GSK_AS_SERVER: (1)	Server sends its public key and cert to client. DNAME = Public RSA key and cert *(1)
GSK_AS_SERVER_WITH_CLIENT_AUTH: (2)	Server sends its public key and cert to client. Client authenticates server's public key and cert. Client checks its local CA-cert file to authenticate. DNAME = public RSA key and cert AND CA-cert for authentication Client sends its public key and cert to server. Server authenticates client's public key and cert. Server checks its local CA-cert file to authenticate. DNAME = public RSA key and cert AND CA-cert for authentication
GSK_AS_CLIENT_NO_AUTH: (3)	Client receives server's public key and cert. Client accepts server's pubic key and cert without authentication. DNAME not used! no RSA key or cert required.

```
// OPTION SYSPARM='66'
// SETPARM IPTRACE='NNNNNNN'
// LIBDEF *,SEARCH=(ssllib.slib,bsilib.slib)
// EXEC BSTTPRXY,SIZE=BSTTPRXY
ID 66
KEYRING PRD2.CONFIG
DNAME BSICERT
SECTYPE TLSV1
OPTION SERVER
PROXY TCP V4 992 SSL * TO V4 23 TXT * LOCALHOST
/*
```

```
// EXEC BSTTPRXY,SIZE=BSTTPRXY,PARM='TRAP(OFF)/'
ID 00
*
KEYRING PRD2.CONFIG
KEYFILE ZVSE51
SECTYPE TLSV1
*
OPTION CLIENT
* 74.125.157.108 IS SMTP.GMAIL.COM
PROXY TCP V4    25 TXT * TO V4   465 SSL * 74.125.157.108
/*
```

```
// EXEC BSTTMTPC,SIZE=BSTTMTPC
ID 00
OPEN 127.0.0.1 25
*
EHLO gmail.com
AUTH LOGIN jeffrey.webmail ????????
MAIL From: <jeffrey.webmail@gmail.com>
RCPT To: <jeff@bsiopti.com>
SUBJ Subject: Test Email
ORGA Organization: Barnard Software, Inc.
*
DATA
*
QUIT
/*
This is a test email text.
See http://www.bsiopti.com

Jeff
/*
```

BSTTATLS

- **BSTTATLS Automatic TLS facility**
- **Automatically converts any application into SSL/TLS application**
- **Transparent to application**

ATLS types

ATLS Types

Source	Destination
Server	Accept SSL connection Convert to clear text for local server application
Client	Accept clear text local client connection Convert to SSL/TLS connection for destination
IPv4 socket	To IPv4 socket
IPv6 socket	To IPv6 socket

Sample ATTLS commands

Sample ATTLS Commands

Command	Description
OPTION CLIENT ATTLS 25 TO SMTP.GOOGLE.COM AS 465 SSL	Intercept outbound CLIENT connections made to SMTP.GMAIL.COM on port 25, convert them to SSL connections on port 465 (Implicit-SMTPS).
OPTION CLIENT OPTION FTP ATTLS 21 TO FTPS.BSIOPTI.COM AS 990 SSL	Intercept outbound FTP CLIENT connections made to FTPS.BSIOPTI.COM on port 21, convert them to SSL connections on port 990 (Implicit-FTPS).
OPTION SERVER ATTLS 23 AS 992 SSL	Intercept inbound SERVER connections made on SSL port 992 (Implicit-TELNETS), convert them to clear text connections on port 23.
OPTION SERVER ATTLS 80 AS 443 SSL	Intercept inbound SERVER connections made on SSL port 443 (Implicit-HTTPS), convert them to clear text connections on port 80.
OPTION SERVER OPTION FTP ATTLS 21 AS 990 SSL	Intercept inbound SERVER connections made on SSL port 990 (Implicit-FTPS), convert them to clear text connections on port 21.

```
// OPTION SYSPARM='00'
// SETPARM IPTRACE='NNNNNNN'
// SETPARM LRGBUF=YES
// LIBDEF *,SEARCH=(ssllib.slib,bsilib.slib)
// EXEC BSTTWAIT,SIZE=BSTTWAIT
/*
// EXEC BSTTATLS,SIZE=BSTTATLS
ID 00
*
KEYRING PRD2.CONFIG
DNAME MYCERT
SECTYPE TLSV1
*
* Convert outbound SMTP connections to Implicit-SMTPS
* but only connections to SMTP.GOOGLE.COM
OPTION CLIENT
ATTLS 25 TO SMTP.GOOGLE.COM AS 465 SSL
*
* Convert Implicit-TELNETS connections to TELNET
OPTION SERVER
ATTLS 23 AS 992 SSL
*
* Convert Implicit-HTTPS connections for CICS TS CWI
OPTION SERVER
ATTLS 80 AS 443 SSL
*
* Convert outbound FTP connections to Implicit-FTPS
OPTION CLIENT
OPTION FTP
ATTLS 21 TO FTPS.BSIOPTI.COM AS 990 SSL
*
* Convert inbound Implicit-FTPS connections to FTP
OPTION SERVER
OPTION FTP
ATTLS 21 AS 990 SSL
/*
```

IPv6/VSE Automatic TLS facility

- **The IPv6/VSE TCP/IP stacks run in separate partitions. The IPv4 stack (BSTTINET) runs in one partition and the IPv6 stack (BSTT6NET) runs in another. The TCP/IP stacks are then coupled together acting as a single stack. The BSTTATLS application is associated with a specific stack (BSTTINET or BSTT6NET). When running a typical dual stack configuration there will be two BSTTATLS application partitions. One for each TCP/IP stack.**
- **The reasons for this design are performance, reliability and robustness. Since the BSTTATLS application is performing SSL/TLS functionality, the overhead of this functionality is offloaded from both the TCP/IP stack and the applications BSTTATLS is servicing.**

Difference between PRXY and ATLS

- **BSTTPRXY is single application**
- **One BSTTPRXY partition for each application**
- **BSTTATLS is multiple application**
- **One BSTTATLS partition for each stack**
- **Each run in their own partition(s)**
- **Better performance, better isolation, better management, more robust**

More information

See http://bsitcpip.blogspot.com/

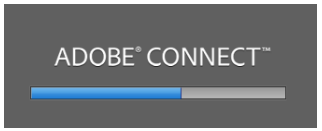
The BSI BLOG!

Questions?

Thank You!

- **Jeffrey Barnard, Barnard Software, Inc.**
- **Joerg Schmidbauer, IBM**

z/VSE Live Virtual Classes



z/VSE @ **http://www.ibm.com/zvse/education/**

LINUX + z/VM + z/VSE @ **http://www.vm.ibm.com/education/lvc/**

Read about upcoming LVCs on  @ **http://twitter.com/IBMzVSE**

Join the LVC distribution list by sending a short mail to stev.glodowski@de.ibm.com