# Encryption Update on z/VSE

Joerg Schmidbauer

http://www.ibm.com/zVSE

http://twitter.com/IBMzVSE

**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.

# Notice Regarding Specialty Engines (e.g., zIIPs, zAAPs and IFLs):

Any information contained in this document regarding Specialty Engines ("SEs") and SE eligible workloads provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g., zIIPs, zAAPs, and IFLs). IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the “Authorized Use Table for IBM Machines” provided at www.ibm.com/systems/support/machine_warranties/machine_code/aut.html (“AUT”).

No other workload processing is authorized for execution on an SE.

IBM offers SEs at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.

# Agenda

New Redbook

News on OpenSSL

APIs

Perfect Forward Secrecy

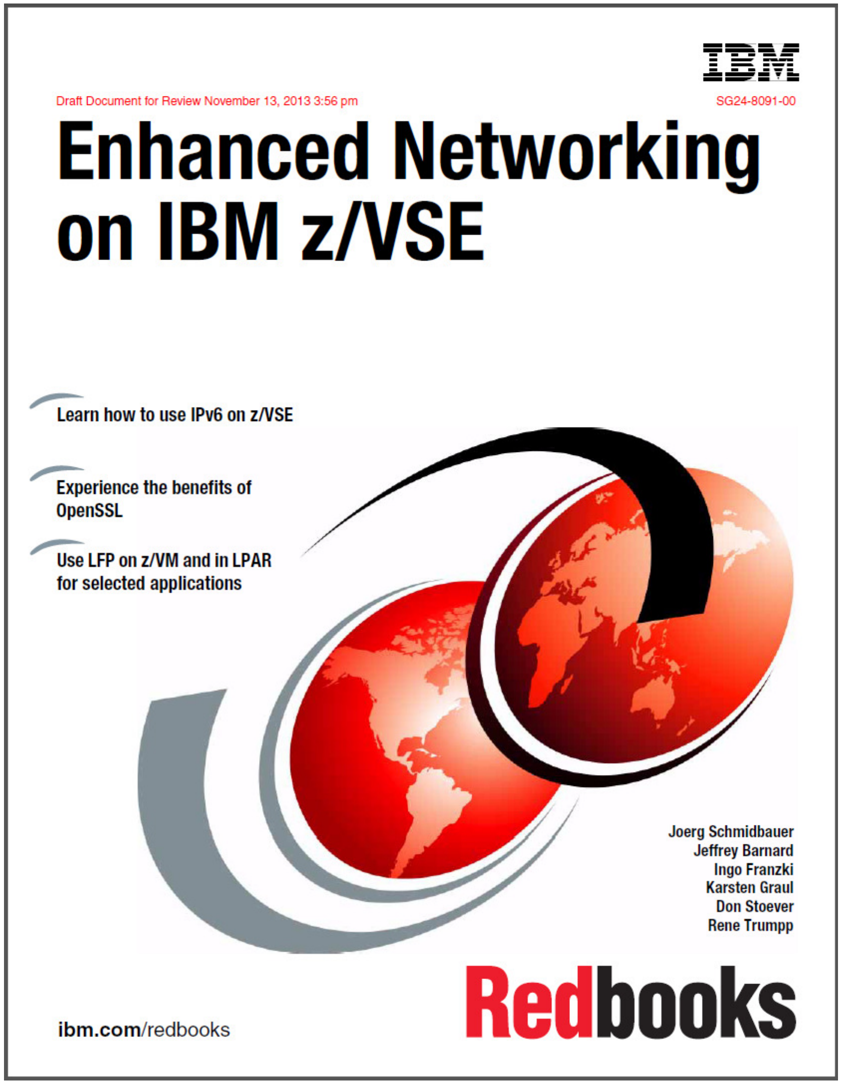
Outlook

# New Redbook

1. Overview on HW and SW
2. TCP/IP for VSE
3. IPv6/VSE
4. Linux Fast Path
5. OpenSSL
6. Comparison of stacks and protocols

Suggestions welcome!

jschmidb@de.ibm.com



IBM

Draft Document for Review November 13, 2013 3:56 pm

SG24-8091-00

Enhanced Networking on IBM z/VSE

Learn how to use IPv6 on z/VSE

Experience the benefits of OpenSSL

Use LFP on z/VM and in LPAR for selected applications

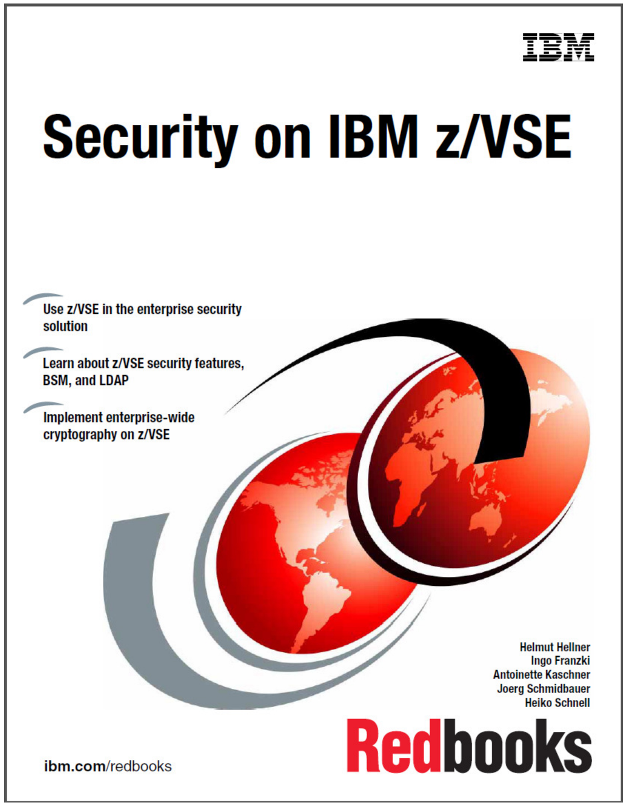
Joerg Schmidbauer
Jeffrey Barnard
Ingo Franzki
Karsten Graul
Don Stoever
Rene Trumpp

Redbooks

ibm.com/redbooks

http://www.redbooks.ibm.com/redpieces/abstracts/sg248091.html?Open

# The two books everyone should read ...



IBM

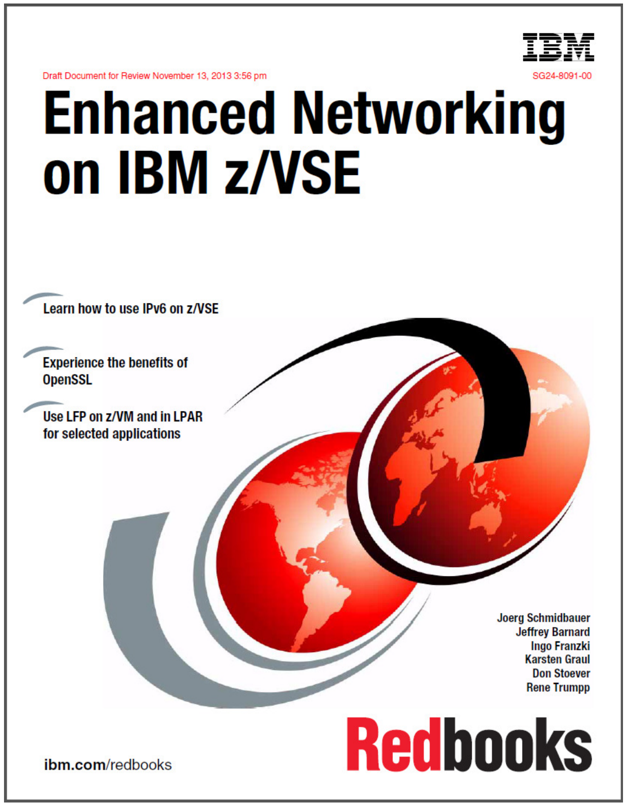
## Security on IBM z/VSE

- Use z/VSE in the enterprise security solution
- Learn about z/VSE security features, BSM, and LDAP
- Implement enterprise-wide cryptography on z/VSE

Helmut Hellner
Ingo Franzki
Antoinette Kaschner
Joerg Schmidbauer
Heiko Schnell

ibm.com/redbooks

Redbooks



IBM

Draft Document for Review November 13, 2013 3:56 pm

SG24-8091-00

## Enhanced Networking on IBM z/VSE

- Learn how to use IPv6 on z/VSE
- Experience the benefits of OpenSSL
- Use LFP on z/VM and in LPAR for selected applications

Joerg Schmidbauer
Jeffrey Barnard
Ingo Franzki
Karsten Graul
Don Stoever
Rene Trumpp

ibm.com/redbooks

Redbooks

# Agenda

New Redbook

News on OpenSSL

APIs

Perfect Forward Secrecy

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/
  http://en.wikipedia.org/wiki/Openssl

OpenSSL: The Open Source toolkit for SSL/TLS - Mozill
File
Edit
View
History
Bookmarks
Tools
Help
www.openssl.org
OpenSSL: The Open Source toolkit f...
+
OpenSSL
Cryptography and SSL/TLS Toolkit
Sponsor OpenSSL | Purchase a Support Contract |
Title
FAQ
About
News
Documents
Source
Contribution

Welcome to the OpenSSL Project

The OpenSSL Project is a collaborative effort to develop a robus full-featured, and Open Source toolkit implementing the Secure v2/v3) and Transport Layer Security (TLS v1) protocols as we general purpose cryptography library. The project is managed by of volunteers that use the Internet to communicate, plan, and deve toolkit and its related documentation.

# OpenSSL on z/VSE

- **Available with z/VSE 5.1 as part of a new system component "z/VSE cryptographic services", 5686-CF9-17-51S**
  - Installed in PRD1.BASE
  - Consists of
    - IJBSSL phase (the OpenSSL functionality)
    - SPEEDTST phase (built-in speed test)
    - NOTICES.Z (License information)
    - IJBSLVSE.OBJ (Access to APIs)
    - IJBSSL.H (function prototypes)
- **Currently used by the IPv6/VSE product from Barnard Software, Inc.**
  - Refer to new Redbook "Enhanced Networking on IBM z/VSE"
  - Some info on OpenSSL is also contained in "z/VSE TCP/IP Support"

# Relevant APARs and PTFs

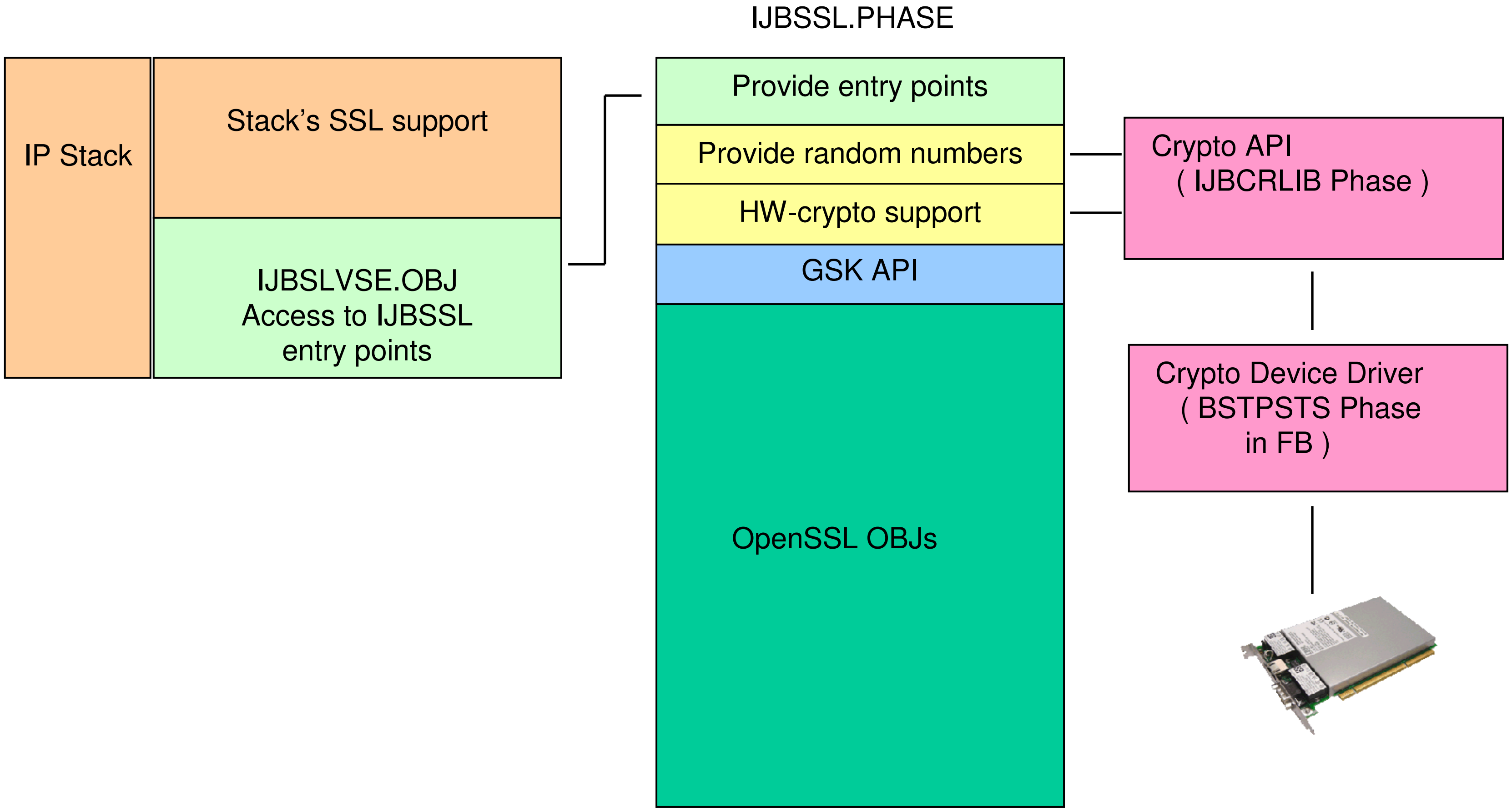
| APAR | PTF | Description | Available since |
|---|---|---|---|
| DY47397 | UD53864 | OpenSSL 1.0.0d update for z/VSE 5.1 | August 2012 |
| DY47414 | UD53863 | VSE/AF update for HW crypto support | August 2012 |
| PM77065 | UK83637 | Initial IPv6/VSE version with OpenSSL support | November 2012 |
| DY47472 | UD53952 | Remove RC4-based cipher suites due to security issues | July 2013 |
| DY47499 | UD53983 | OpenSSL 1.0.1e update | December 2013 |
| PM98875 | UK98397 | IPv6/VSE update for TLSv1.2 support | December 2013 |

# Specifics for OpenSSL on VSE

- **Restrictions**
  - The openssl command line tool is not available on VSE.
  - Keystores (PEM files) are created on a PC and then uploaded to VSE. This is supported by the Keyman/VSE tool: http://www.ibm.com/systems/z/os/zvse/downloads/#vkeyman
  - Some algorithms excluded due to legal reasons
  - Currently only for LE/C
- **Only available on z/VSE**
  - Hardware Crypto Support: Crypto Express cards and CPACF
  - SSL API is compatible to z/OS SSL API (*) and CSI SSL API, i.e. existing VSE SSL applications can run unchanged with OpenSSL (LE/C only).
  - OpenSSL Trace

(*) Refer to: *z/OS Cryptographic Services, SSL Programming*, SC24-5901 and *z/VSE TCP/IP Support*, SC34-2640

# OpenSSL integration in z/VSE



IJBSSL.PHASE

IP Stack

Stack's SSL support

IJBSLVSE.OBJ
Access to IJBSSL
entry points

Provide entry points

Provide random numbers

HW-crypto support

GSK API

OpenSSL OBJs

Crypto API
( IJBCRLIB Phase )

Crypto Device Driver
( BSTPSTS Phase
in FB )

# Upgrade to OpenSSL 1.0.1e

- OpenSSL 1.0.1e is the currently latest service level on openssl.org (from Feb 2013)
- Provides new functionality and bug fixes, especially
  - Support of TLSv1.2
- OpenSSL 1.0.1e available on VSE since Dec 2013
  - APAR DY47499 / PTF UD53983
- Latest IPv6/VSE PTF contains code to support the new TLSV1.2 parameter

The following slides explain the advantage of TLS v1.2 and why you should upgrade to this protocol version.

# What is TLS v1.2

- **TLSv1.2 is the currently latest SSL protocol version, after**
  - SSL 3.0
  - TLS 1.0
  - TLS 1.1
- **TLSv1.2 provides new SSL cipher suites**
  - `0x3B    TLS_RSA_WITH_NULL_SHA256`
  - `0x3C    TLS_RSA_WITH_AES_128_CBC_SHA256`
  - `0x3D    TLS_RSA_WITH_AES_256_CBC_SHA256`
- **TLSv1.2 is described in RFC 5246**
  - http://tools.ietf.org/html/rfc5246

What’s the difference to the previously available cipher suites?

# Comparison

- **Available ciphers so far**
  - SSL_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
    -

They all use the SHA-1 algorithm

- **TLSv1.2**
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA256

These use SHA-256

OK, first of all, what is a hash function?

# What is a hash function?

- **A cryptographic hash function takes an arbitrary block of data and returns a fixed-size bit string, the *cryptographic hash value, sometimes also called "fingerprint"* or "message digest".**
- **It has these main properties:**
  - it is easy to compute the hash value for any given message
  - it is infeasible to generate a message that has a given hash
  - it is infeasible to modify a message without changing the hash
  - it is infeasible to find two different messages with the same hash.

OK, what's the difference between SHA-1 and SHA-256?

Source: http://en.wikipedia.org/wiki/Hash_function_%28cryptography%29

# Comparison SHA-1 versus SHA-256

- **SHA-1**
  - Maximum input length = approx. $2^{64}$ Bits = approx. 2 Exabyte = 2 Mio TB = 500.000 Cartridges of 4 TB, e.g. for TS1140 tape drive
  - Hash value has 160 Bits = 20 Bytes
- **SHA256**
  - Maximum input length = $2^{128}$ Bits
  - Hash value has 256 Bits = 32 Bytes

Is SHA-1 not enough?

Source: http://en.wikipedia.org/wiki/Secure_hash_algorithm

# SHA-1 discussion

- **In 2005 a team of three Chinese researchers published an attack on simplified versions of SHA-1.**
  - http://en.wikipedia.org/wiki/SHA-1
- **From Bruce Schneier‘s blog in Feb 2005:**
  - Jon Callas, PGP's CTO, put it best: "It's time to walk, but not run, to the fire exits. You don't see smoke, but the fire alarms have gone off." That's basically what I said last August. It's time for us all to migrate away from SHA-1.
  - https://www.schneier.com/blog/archives/2005/02/sha1_broken.html

Ok, this does not sound very urgent ...

# NIST Special Publication 800-131A

- **NIST = National Institute of Standards and Technology**
  - Part of the U.S. Department of Commerce
- ***NIST Special Publication 800-131A*** **dated January 2011 entitled "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths" Table 9 states that the use of the SHA-1 hash function is disallowed after December 31, 2013 except for non-digital signature applications.**
- **Source:**
  - http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

… well, the NIST already changed their recommendations.

# Agenda

New Redbook

News on OpenSSL

APIs

Perfect Forward Secrecy

Outlook

# API support

| | SSL API | Crypto API |
|---|---|---|
| LE/C sockets | Yes (C only) | - |
| EZASMI / EZASOKET | Yes (ASM, COBOL, PL/1) | - |
| TCP/IP for VSE | Yes (ASM and C) | Yes (ASM and C) |
| OpenSSL | Yes (C only)<br>Non-C: TODO! | Yes (C only)<br>Non-C: TODO! |
| CPACF | - | Yes (ASM *) |

(*) Refer to "Principles of Operation", instructions KM, KMC, KMF, etc.

# Agenda

New Redbook

News on OpenSSL

APIs

Perfect Forward Secrecy

Outlook

# First some terms …

- **Short-term keys**
  - Are usually keys for symmetric encryption algorithms like DES, Triple-DES, AES.
  - Are often called „session keys“, „data keys“, or „encryption keys“.
  - Are used to encrypt the data.
  - Are generated either by random or from a given password
- **Long-term keys**
  - Are usually public / private RSA key pairs.
  - Are typically used in SSL to transfer/protect short-term keys.
  - Are sometimes called „key-encrypting keys“
  - Are sometimes used for protecting session keys when creating encrypted backups. Hereby one or more session keys are encrypted with different long-term keys and stored in the backup together with the data.

# Perfect Forward Secrecy (PFS)

- **From Wikipedia:**
  - “PFS is a property of key-agreement protocols that ensures that a session key derived from a set of long-term keys will not be compromised if one of the long-term keys is compromised in the future”.

**… in other words:** even if a long-term key is compromised in future, it is not possible to get access to a session key, and thus, to the data.

- **Implication:**
  - In PFS, session keys are not protected (encrypted) by long-term keys (e.g. RSA private/public keys).

Source: http://en.wikipedia.org/wiki/Perfect_Forward_Secrecy

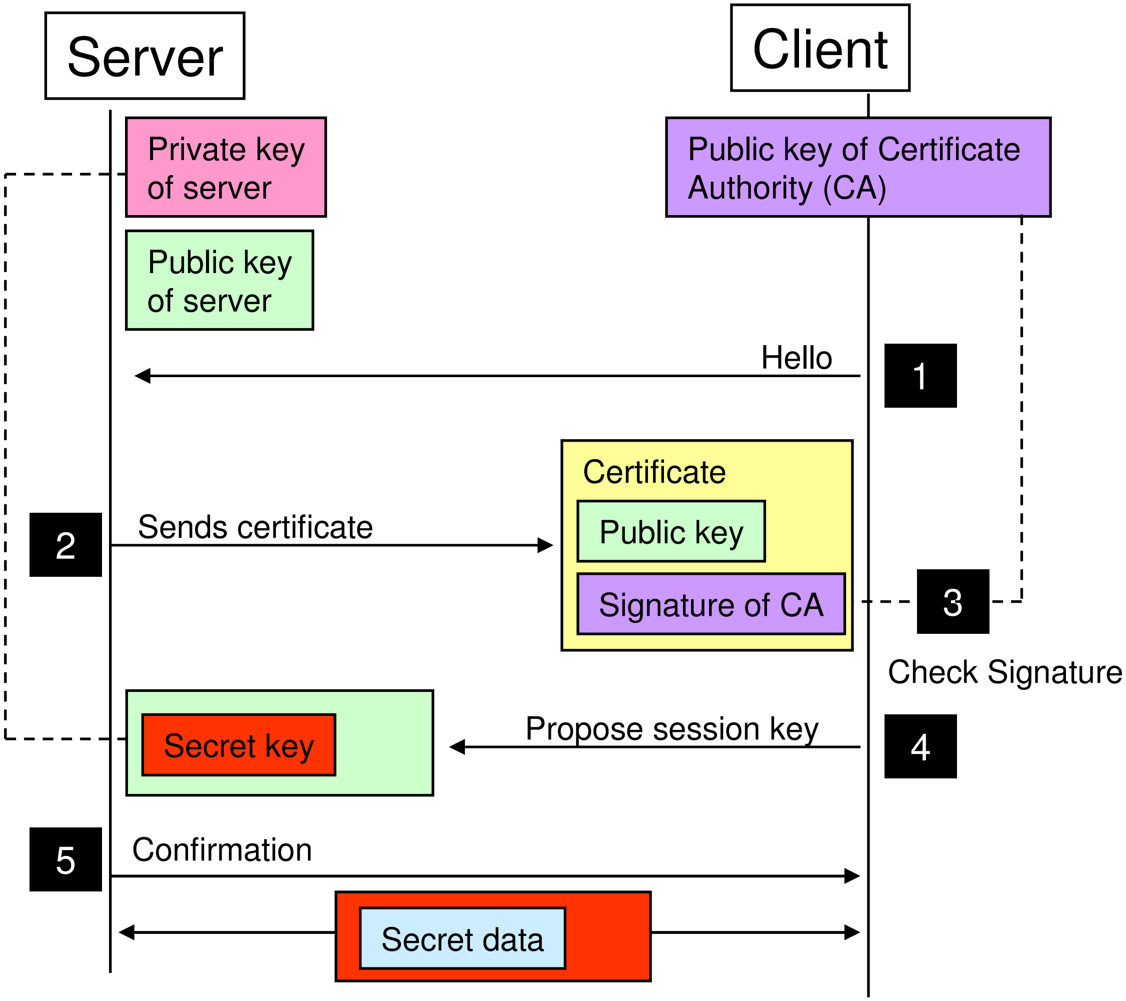
# Major difference between RSA and PFS

- **RSA**
  - A randomly generated session key gets encrypted with an RSA public key and is part of the network session data or encrypted backup.
- **PFS**
  - Uses the Diffie-Hellman (DH) key agreement method where a session key is never part of a network session.
  - PFS is not applicable for encrypted backups, only secure network connections are considered.

OK, but how does it work?

# Case 1: Session establishment with RSA

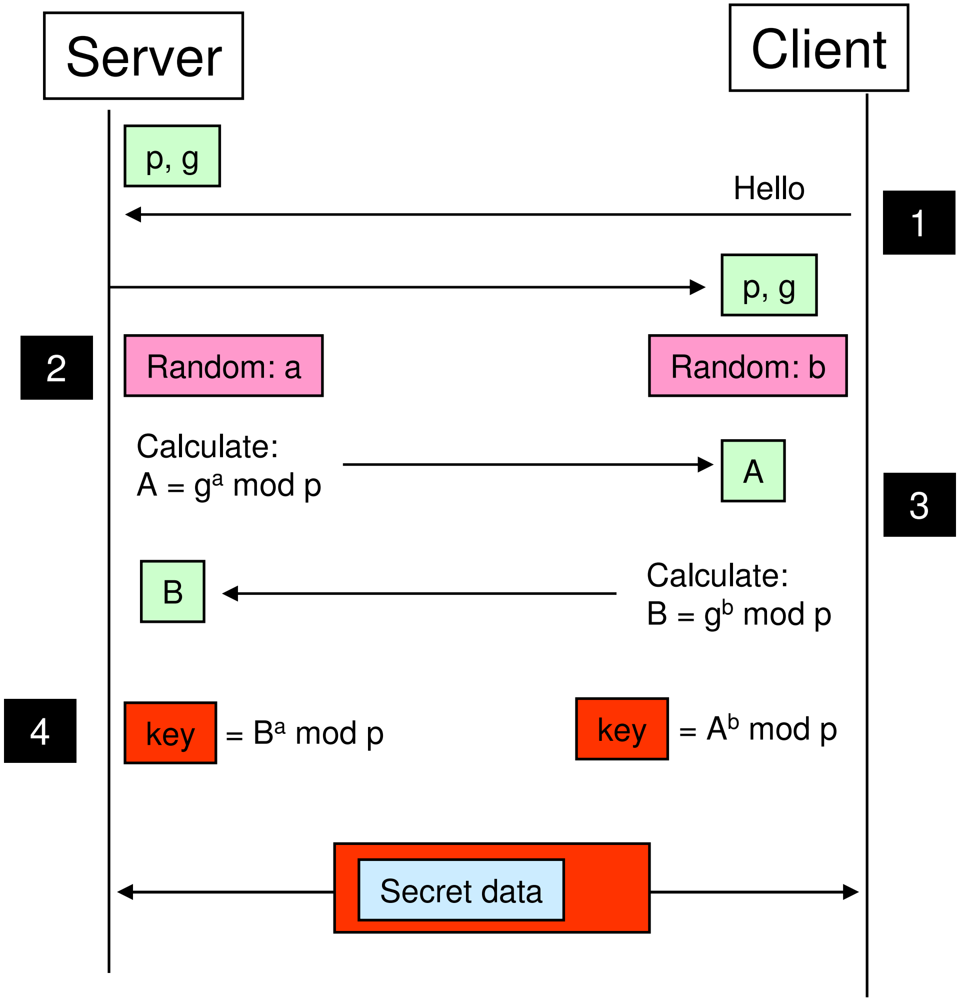
1. Browser contacts https://my-bank.com
2. Server sends public key wrapped into a digital certificate, signed by a trusted Certificate Authority (CA).
3. Browser checks signature of the CA and assumes to be in fact connected to my-bank.com. From now on the Browser encrypts messages with the server's public key. Server can decrypt these messages with its corresponding private key.
4. Browser proposes a secret session key, encrypted by the server's public key. Here we have the weakness.
5. Server confirms the secret session key.



# Case 2: session establishment with DH

1. The communication partners agree on two values p and g (DH parameters). There is a mathematical relationship between these two values.
2. Both parties generate a random number in the range {1 ... p-2}. These two numbers are never sent over the line.
3. Both parties perform certain calculations to derive two values A and B, which are exchanged over the unsecure medium.
4. Both parties can now derive the same secret key. This key is never part of the connection data.

Authentication not considered here!



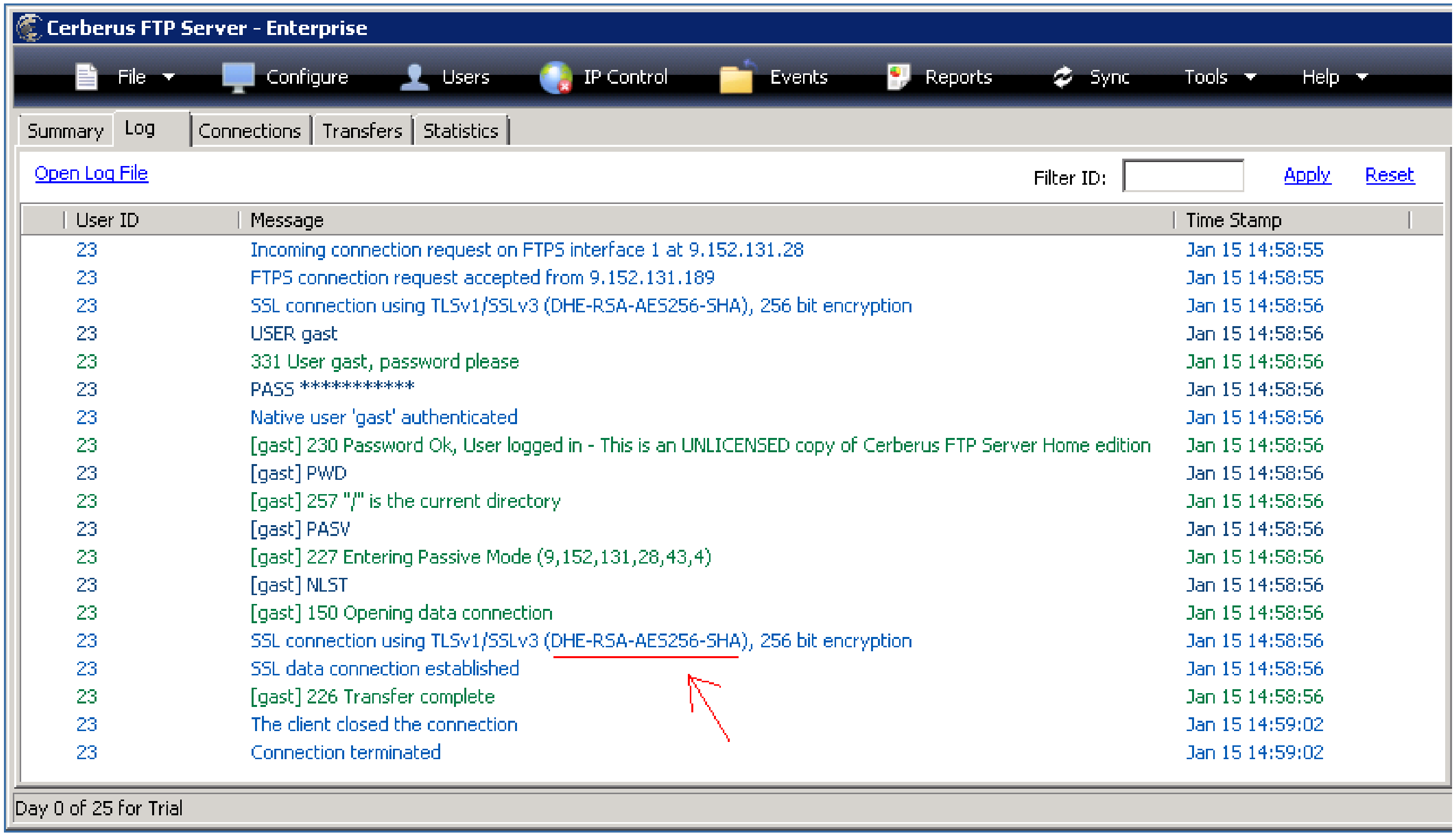
Source: http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

# Pro’s and Con’s

- **RSA**
  - Well established and supported by almost all web sites
  - Big RSA key sizes guarantee desired level of security, but:
  - Huge processing overhead with 2048-bit and 4096-bit keys
- **Diffie-Hellman**
  - DH parameters need a long time to generate, but can be created in advance
  - In practice, authentication via certificates is added to the DH key exchange method
  - Also significant processing overhead when opening a connection
  - Currently supported only by few sites, e.g. Google gmail

# DH with OpenSSL on VSE

- Latest OpenSSL code on VSE can do Diffie-Hellman!
- Example: BSTTFTPC (FTP client), Cerberus FTP Server



| User ID | Message | Time Stamp |
|---|---|---|
| 23 | Incoming connection request on FTPS interface 1 at 9.152.131.28 | Jan 15 14:58:55 |
| 23 | FTPS connection request accepted from 9.152.131.189 | Jan 15 14:58:55 |
| 23 | SSL connection using TLSv1/SSLv3 (DHE-RSA-AES256-SHA), 256 bit encryption | Jan 15 14:58:56 |
| 23 | USER gast | Jan 15 14:58:56 |
| 23 | 331 User gast, password please | Jan 15 14:58:56 |
| 23 | PASS *********** | Jan 15 14:58:56 |
| 23 | Native user 'gast' authenticated | Jan 15 14:58:56 |
| 23 | [gast] 230 Password Ok, User logged in - This is an UNLICENSED copy of Cerberus FTP Server Home edition | Jan 15 14:58:56 |
| 23 | [gast] PWD | Jan 15 14:58:56 |
| 23 | [gast] 257 "/" is the current directory | Jan 15 14:58:56 |
| 23 | [gast] PASV | Jan 15 14:58:56 |
| 23 | [gast] 227 Entering Passive Mode (9,152,131,28,43,4) | Jan 15 14:58:56 |
| 23 | [gast] NLST | Jan 15 14:58:56 |
| 23 | [gast] 150 Opening data connection | Jan 15 14:58:56 |
| 23 | SSL connection using TLSv1/SSLv3 (DHE-RSA-AES256-SHA), 256 bit encryption | Jan 15 14:58:56 |
| 23 | SSL data connection established | Jan 15 14:58:56 |
| 23 | [gast] 226 Transfer complete | Jan 15 14:58:56 |
| 23 | The client closed the connection | Jan 15 14:59:02 |
| 23 | Connection terminated | Jan 15 14:59:02 |

http://www.cerberusftp.com/

# Agenda

New Redbook

News on OpenSSL

APIs

Perfect Forward Secrecy

Outlook

# Outlook

- **Customers are replacing their 1024-bit RSA keys by 2048-bit keys since years**
  - Note: 2048-bit keys require Crypto Express hardware. TCP/IP for VSE cannot process 2k keys in software. OpenSSL can do this, but does not perform.
- **Customers will over time migrate to TLSv1.2 and use the SHA-256 based SSL cipher suites.**
- **The Diffie-Hellman key agreement method will get wider use, first of all in security-critical applications.**
  - Hopefully Online Banking ...
- **Regular updates on OpenSSL help reducing security risks**

# Thank You

Please forward your questions or remarks to
zvse@de.ibm.com
jschmidb@de.ibm.com

# 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 alina.glodowski@de.ibm.com