



IBM Ported Tools for z/OS Version 1.3 updated to include new level of Open SSH, 6.4p1

Table of contents

1 Overview	4 Technical information
2 Key prerequisites	4 Ordering information
2 Planned availability date	6 Terms and conditions
2 Statement of general direction	8 Prices
3 Program number	9 Announcement countries
3 Publications	

At a glance

For Version 1 Release 3 of the IBM^(R) Ported Tools for z/OS^(R) product, the base is updated to include a new level of Open SSH, 6.4p1. OpenSSH 6.4p1 follows IETF Secsh RFCs.

Overview

IBM Ported Tools for z/OS, a program product available at no cost to you, is designed to deliver UNIXTM ported tools and utilities that are modified to operate within the z/OS environment. These tools and utilities are useful for application development on, and secure communications to, the z/OS platform. For Version 1 Release 3 of the IBM Ported Tools for z/OS product, the base is updated to include a new level of Open SSH, 6.4p1.

With Open SSH 6.4p1, significant new features include:

- Elliptic-curve DSA (ECDSA) public key (both user and host) support.
- Support for new Gallois-Curve Mode (GCM) cipher algorithms with AES encryption.
- Support for SHA-2 MACs.
- Support for "Encrypt-then-MAC" (ETM) mode for existing MAC algorithms, which is considered to be more secure.
- Dynamic port assignment for report port forwarding. A remote port of "0" can be specified, in which case a dynamic port will be assigned on the server. The client will report a message with the specific port assigned.
- More flexibility in configuration files: Conditional *Match* blocks have more criteria and can include more options within the block.
- Support for public key (user and host) certificates. These are not X.509 certificates, but a simpler implementation that is unique to SSH.
- SFTP client and server support for recursively transferring files in a directory tree.
- Multiple user authentication methods. Users can be required to authenticate with more than one method (password, public key, and so on).
- Elimination of ssh-rand-helper. Instead, the Integrated Cryptographic Service Facility (ICSF) component of the z/OS Cryptographic Services, a base element of z/OS, is now used for secure random number generation. Hence, the ICSF component needs to be operational for use by IBM Ported Tools for z/OS, V1.3.

OpenSSH 6.4p1 follows IETF Secsh RFCs, including:

- The Secure Shell (SSH) Protocol Assigned Numbers, RFC 4250, 2006
- The Secure Shell (SSH) Protocol Architecture, RFC 4251, 2006
- The Secure Shell (SSH) Authentication Protocol, RFC 4252, 2006
- The Secure Shell (SSH) Transport Layer Protocol, RFC 4253, 2006
- The Secure Shell (SSH) Connection Protocol, RFC 4254, 2006
- Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints, RFC 4255, 2006
- Generic Message Exchange Authentication for the Secure Shell Protocol (SSH), RFC 4256, 2006
- The Secure Shell (SSH) Session Channel Break Extension, RFC 4335, 2006
- The Secure Shell (SSH) Transport Layer Encryption Modes, RFC 4344, 2006
- Improved Arcfour Modes for the Secure Shell (SSH) Transport Layer Protocol, RFC 4345, 2006
- Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol, RFC 4419, 2006
- The Secure Shell (SSH) Public Key File Format, RFC 4716, 2006
- Elliptic Curve Algorithm Integration in SSH, RFC 5656, 2009
- SHA-256 SSHFP Resource Records in DNS, RFC 6594, 2012
- SHA-2 Data Integrity Algorithms, RFC 6668, 2012

In addition, the following z/OS enhancements are available:

- Updates to SMF record processing: The SMF record associated when file transfers are completed by the SFTP client and will now contain the target file path name.
- New SMF record subtypes record will be written after successful negotiation and authentication of an SSH client or server session. This improves your ability to monitor and report on additional details, such as algorithms being used.
- The ssh client command will be enabled to run under TSO OMVS (3270), but prompting for passwords or pass phrases will not be allowed.
- Support for hardware-accelerated AES CTR-mode ciphers, which can help reduce CPU utilization.

Key prerequisites

IBM Ported Tools for z/OS, Version 1.3.0 requires installation of z/OS V1.13 (5694-A01), or later.

Planned availability date

February 20, 2015

Availability of programs with encryption algorithm in France is subject to French government approval.

Statement of general direction

In z/OS V2.2, the Open SSH is planned to be provided as a base element. See Software Announcement [ZP15-0006](#), dated January 14, 2015.

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver

any material, code, or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remain at our sole discretion.

Reference information

Refer to Software Announcement [ZP14-0052](#), dated February 4, 2014.

Program number

Program number	VRM	Program name
5655-M23	1.3.0	IBM Ported Tools for z/OS

Product identification number

Program PID number	Subscription and Support PID number
5655-M23	5655-M29

Offering Information

Product information is available via the Offering Information website

<http://www.ibm.com/common/ssi>

Publications

The following publications are supplied automatically with the basic machine-readable material:

Title	Order number
IBM Ported Tools for z/OS Program Directory	GI10-0769
IBM Ported Tools for z/OS License Information	GA22-7986

Displayable softcopy publications

The IBM Ported Tools for z/OS, V1.3.0 documentation is available at

<http://www.ibm.com/systems/z/os/zos/features/unix/ported/>

The IBM Publications Center

<http://www.ibm.com/shop/publications/order>

The Publications Center is a worldwide central repository for IBM product publications and marketing material with a catalog of 70,000 items. Extensive search facilities are provided. Payment options for orders are via credit card (in the US) or customer number for 20 countries. A large number of publications are available online in various file formats, and they can all be downloaded by all countries, free of charge.

Services

Global Technology Services

Contact your IBM representative for the list of selected services available in your country, either as standard or customized offerings for the efficient installation, implementation, or integration of this product.

Technical information

Specified operating environment

Hardware requirements

IBM Ported Tools for z/OS, V1.3.0 is compatible with all hardware as listed in the compatibility statements of z/OS V1.13 (5694-A01) or later systems.

Software requirements

IBM Ported Tools for z/OS, V1.3.0 requires z/OS V1.13 (5694-A01) or later systems.

The program's specifications and specified operating environment information may be found in documentation accompanying the program, if available, such as a readme file, or other information published by IBM, such as an announcement letter. Documentation and other program content may be supplied only in the English language.

Security, auditability, and control

IBM Ported Tools for z/OS uses the security and auditability features of the z/OS operating system.

The customer is responsible for evaluation, selection, and implementation of security features, administrative procedures, and appropriate controls in application systems and communication facilities.

Ordering information

Consult your IBM representative.

Ordering z/OS through the Internet

ShopzSeries provides an easy way to plan and order your z/OS ServerPac or CBPDO. It will analyze your current installation, determine the correct product migration, and present your new configuration based on z/OS. Additional products can also be added to your order (including determination of whether all product requisites are satisfied). ShopzSeries is available in the US and several countries in Europe. In countries where ShopzSeries is not available yet, contact your IBM representative (or IBM Business Partner) to handle your order via the traditional IBM ordering process. For more details and availability, visit the ShopzSeries website at

<http://www14.software.ibm.com/webapp/ShopzSeries/ShopzSeries.jsp>

5655-M23 - IBM Ported Tools for z/OS

Charge metric

This is a no-charge product.

Basic license

To order, specify the program product number and the appropriate license or charge option. Also, specify the desired distribution medium. To suppress shipment of media, select the license-only option in CFSW.

Program name: IBM Ported Tools for z/OS

Program PID: 5655-M23

Entitlement identifier	Description	License option/Pricing metric
S0114M7	IBM Ported Tools for z/OS	No Charge, Unlimited installs
Orderable supply ID	Language	Distribution medium
S0165V9	English	3590

Subscription and Support PID: 5655-M29

Entitlement identifier	Description	License option/Pricing metric
S0114V1	IBM Ported Tools for z/OS S&S	No Charge, Unlimited installs SW Subscription and Support Registration
Orderable supply ID	Language	Distribution medium
S0114V2	English	Paper

Program name: IBM Ported Tools: HTTP Server

Program PID: 5655-M23

Entitlement identifier	Description	License option/Pricing metric
S0159D2	IBM Ported Tools: HTTP Server	No Charge, Unlimited installs
Orderable supply ID	Language	Distribution medium
S0165VD	English	3590

Subscription and Support PID: 5655-M29

Entitlement identifier	Description	License option/Pricing metric
S015D46	IBM HTTP Server S&S	No Charge, Unlimited installs SW Subscription and Support Registration
Orderable supply ID	Language	Distribution medium
S015D45	English	Paper

Customized Offerings

Product deliverables are shipped only via CBPDO, ServerPac, SystemPac, FunctionPac, and ProductPac^(R).

All of these customized offerings are offered for Internet delivery in countries where Shopz product ordering is available. Internet delivery reduces software delivery time and allows you to install software without the need to handle tapes. For more details on Internet delivery, refer to the Shopz help information at

<http://www.software.ibm.com/ShopzSeries>

You choose the delivery method when you order the software. IBM recommends Internet delivery. In addition to Internet and DVD, the supported tape delivery options include:

- 3590
- 3592

Most products can be ordered in ServerPac, SystemPac, FunctionPac, and ProductPac the month following their availability in CBPDO. z/OS can be ordered via CBPDO, ServerPac, and SystemPac at general availability. Many products will also be orderable in a Product ServerPac without also having to order the z/OS operating system or subsystem. Shopz and CFS W will determine the eligibility based on product requisite checking. For more details on the product ServerPac, visit the Help section on the Shopz website at

<http://www14.software.ibm.com/webapp/ShopzSeries/ShopzSeries.jsp>

For additional information on the Product ServerPac option, refer to Software Announcement [ZP12-0358](#), dated July 31, 2012.

Production of software product orders will begin on the planned general availability date.

- CBPDO shipments will begin one week after general availability.
- ServerPac shipments will begin two weeks after general availability.
- SystemPac, FunctionPac and ProductPac shipments will begin four weeks after general availability due to additional customization, and data input verification.

Terms and conditions

The information provided in this announcement letter is for reference and convenience purposes only. The terms and conditions that govern any transaction with IBM are contained in the applicable contract documents such as the IBM International Program License Agreement, IBM International Passport Advantage^(R) Agreement, and the IBM Agreement for Acquisition of Software Maintenance.

Licensing

IBM International Program License Agreement including the License Information document and Proof of Entitlement (PoE) govern your use of the program. PoEs are required for all authorized use.

Agreement for Acquisition of Software Maintenance

The following agreement applies for Software Subscription and Support (Software Maintenance) and does not require customer signatures:

- IBM Agreement for Acquisition of Software Maintenance (Z125-6011)

These programs are licensed under the IBM Program License Agreement (IPLA) and the associated Agreement for Acquisition of Software Maintenance, which provide for support with ongoing access to releases and versions of the program. These programs have a one-time license charge for use of the program and an annual renewable charge for the enhanced support that includes telephone assistance (voice support for defects during normal business hours), as well as access to updates, releases, and versions of the program as long as support is in effect. IBM System z^(R) Operational Support Services - SoftwareXcel is an option if you desire added services.

License Information number

GA22-7986

The program's License Information will be available for review on the IBM Software License Agreement website

<http://www.ibm.com/software/sla/sladb.nsf>

Limited warranty applies

Yes

Limited warranty

IBM warrants that when the program is used in the specified operating environment, it will conform to its specifications. The warranty applies only to the unmodified portion of the program. IBM does not warrant uninterrupted or error-free operation of the program or that IBM will correct all program defects. You are responsible for the results obtained from the use of the program.

IBM provides you with access to IBM databases containing information on known program defects, defect corrections, restrictions, and bypasses at no additional charge. For further information, consult the IBM Software Support Handbook found at

<http://www.ibm.com/support/handbook>

IBM will maintain this information for at least one year after the original licensee acquires the program (warranty period).

Money-back guarantee

If for any reason you are dissatisfied with the program and you are the original licensee, you may obtain a refund of the amount you paid for it, if within 30 days of your invoice date you return the program and its PoE to the party from whom you obtained it. If you downloaded the program, you may contact the party from whom you acquired it for instructions on how to obtain the refund.

For clarification, note that for programs acquired under any of IBM's On/Off Capacity on Demand (On/Off CoD) software offerings, this term does not apply since these offerings apply to programs already acquired and in use by you.

Volume orders (IVO)

No

Passport Advantage applies

No

Software Subscription and Support applies

For operating system software, the revised IBM Operational Support Services - Support Line offering will provide support for those operating systems and associated products that are not available with the Software Subscription and Support (Software Maintenance) offering.

This will ensure total support coverage for your enterprise needs, including IBM and selected non-IBM products. For complete lists of products supported under both the current and revised offering, visit

System i Software Maintenance applies

No

Variable charges apply

No

Educational allowance available

Yes. When ordering through the program number process, a 15% education allowance applies to qualified education institution customers.

Education Software Allowance Program applies when ordering through the program number process.

ESAP available

Yes, to qualified customers.

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, or misappropriated or can result in misuse of your systems to attack others. Without a comprehensive approach to security, no IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products, or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

Prices

For all local charges, contact your IBM representative.

The prices are unchanged by this announcement.

IBM Global Financing

IBM Global Financing offers competitive financing to credit-qualified customers to assist them in acquiring IT solutions. Offerings include financing for IT acquisition, including hardware, software, and services, from both IBM and other manufacturers or vendors. Offerings (for all customer segments: small, medium, and large enterprise), rates, terms, and availability can vary by country. Contact your local IBM Global Financing organization or visit

<http://www.ibm.com/financing>

IBM Global Financing offerings are provided through IBM Credit LLC in the United States, and other IBM subsidiaries and divisions worldwide to qualified commercial and government customers. Rates are based on a customer's credit rating, financing terms, offering type, equipment type, and options, and may vary by country. Other

restrictions may apply. Rates and offerings are subject to change, extension, or withdrawal without notice.

For more financing information, visit

<http://www.ibm.com/financing>

Announcement countries

All European, Middle Eastern, and African countries.

Trademarks

IBM, z/OS, Global Technology Services, Passport Advantage, System i, ProductPac and System z are registered trademarks of IBM Corporation in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Terms of use

IBM products and services which are announced and available in your country can be ordered under the applicable standard agreements, terms, conditions, and prices in effect at the time. IBM reserves the right to modify or withdraw this announcement at any time without notice. This announcement is provided for your information only. Reference to other products in this announcement does not necessarily imply those products are announced, or intend to be announced, in your country. Additional terms of use are located at

[Terms of use](#)

For the most current information regarding IBM products, consult your IBM representative or reseller, or visit the IBM worldwide contacts page

<http://www.ibm.com/planetwide/>