Trusting Your Code

A deep-dive into Guest Secure IPL, Digital Signature Verification, and what all this cryptography even means

Brian Hugenbruch, CISSP
bwhugen@us.ibm.com
z/VM Development
Endicott, NY, US*

Arielle Goldberg
arielle.goldberg1@ibm.com
z/VM Development
Poughkeepsie, NY, US

A
VM Workshop
Original
Presentation

***ish**

Agenda

Introduction

Problem statement

Digital Signatures?

Validating your Service

Validating your Guests

Validating the Future

Q&A

Who we are

Brian Hugenbruch, CISSP

- IBM Endicott | Poughkeepsie
- z/VM Development (~24 years)
- z/VM Security Nerd (~15 years)
- Knight of VM (Class of 2017)
- Fun facts:
  - Two-time VM chili contest winner
  - NCAA Division I Varsity Fencer
  - Member of SFWA
  - Preferred Ice Cream flavor: Peach bourbon

Arielle Goldberg

- IBM Poughkeepsie
- z/VM Development (~2.5 years)
- Fun facts:
  - Played ultimate frisbee with Bill Nye
  - Released an indie video game
  - Spent a summer learning the bagpipes
  - Mega champion of Just Dance ABBA
  - Preferred Ice Cream flavor: cookie dough

Why are we here?

It might sound obvious, but especially in a large enterprise, **the number of rules** to which you must adhere is non-trivial

- *Just because no one's told you about the rules does not mean they're not there.*

In an ideal world, you start with the rules and then build the system

When inheriting architecture, this isn't always possible

Step 1: know your system

Step 2: know the technology

Step 3: know your requirements

z/VM Security Certifications

z/VM releases not listed are "designed to conform to the standards of each security evaluation."

z/VM Level	Common Criteria	
z/VM 7.4	*Announced – coming in ~3Q2024*	
z/VM 7.3	*Not evaluated (“designed to conform to standards”)*	
z/VM 7.2	***BSI OSPP (with Virt and Labeled Security extensions) at EAL 4+ – Completed!***	***NIAP VPP with Server Virt. Extended Package – Completed!***
z/VM 7.1	*Not evaluated (“designed to conform to standards”)*	
z/VM 6.4	OSPP with Labeled Security and Virtualization at EAL 4+ -- ***COMPLETED!*** *http://www.ocsi.isticom.it/index.php/elenchi-certificazioni/in-corso-di-valutazione*	

z/VM Level	FIPS 140-n
z/VM 7.4	*Announced – coming in 3Q2024*
z/VM 7.3	*Not evaluated (“designed to conform to standards”)*
z/VM 7.2	***FIPS 140-2 L1 for z/VM System SSL and ICSFLIB – Completed!***
z/VM 7.1	*Not evaluated (“designed to conform to standards”)*
z/VM 6.4	FIPS 140-2 L1 – ***COMPLETED!*** *https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3374*

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

…there are more rules than you think.

- *Supply chain attacks have led to an increase in security focus on software build*

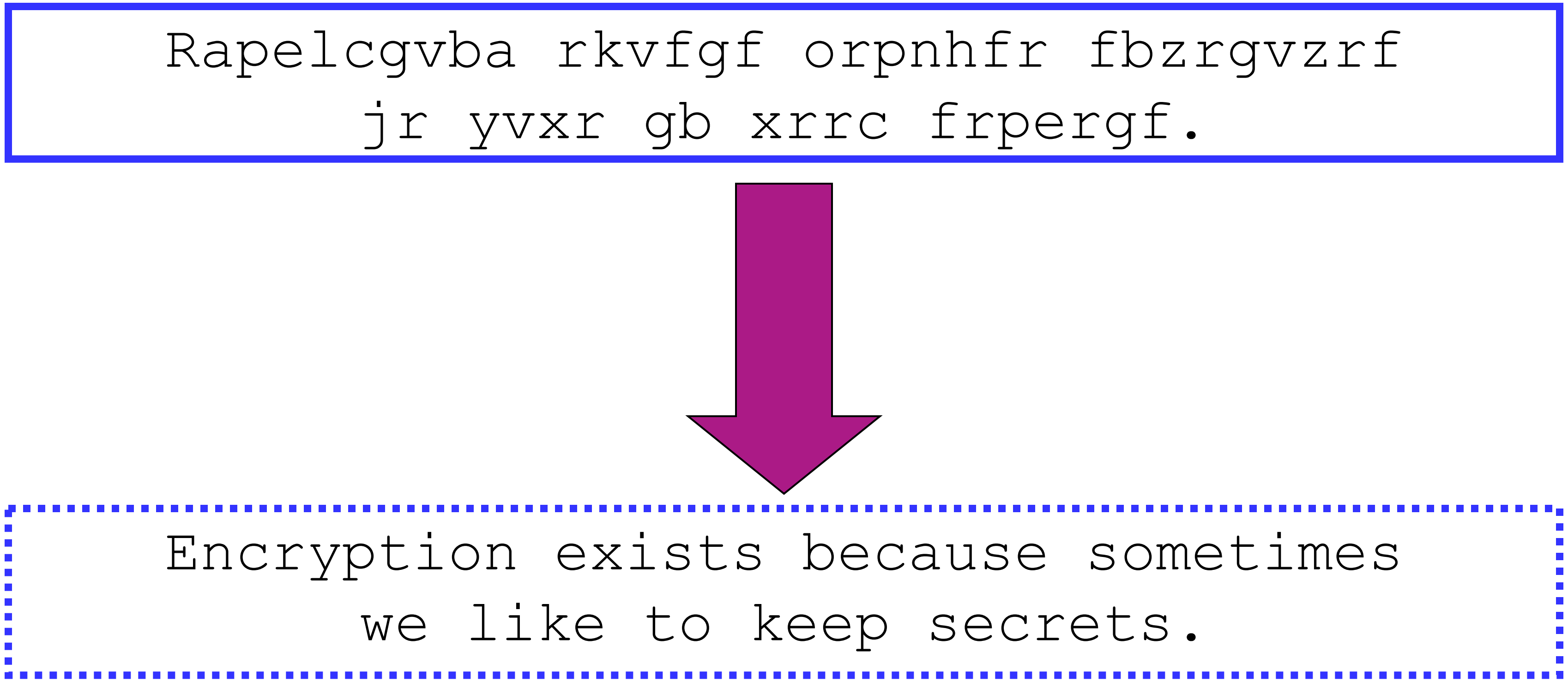
- *IBM has already delivered functions to that end*
  - IBM Z Secure Service Containers and HyperProtect Services
  - z15 Secure IPL (for Linux in an LPAR)
  - z16 List-Directed Secure IPL (for Linux and z/OS)
  - z/VM Guest Secure IPL (z16)
  - Digital signing of IBM service (z/VM and z/OS)
  - Digital signature verification of IBM service (for z/VM, just recently, via GETSHOPZ)

- *Which is good, because modern requirements are bringing such things into their must-do lists*
  - NIAP OSPP and NIAP VPP (Common Criteria)
  - White House Executive Order on Improving Cyber Security (2021 and related)
  - NIS2 / DORA (EU)

- *Goal is to use digital signatures to validate both authenticity and integrity of the code you IPL*

So what is a digital signature?

(Math. It’s lots of math.)



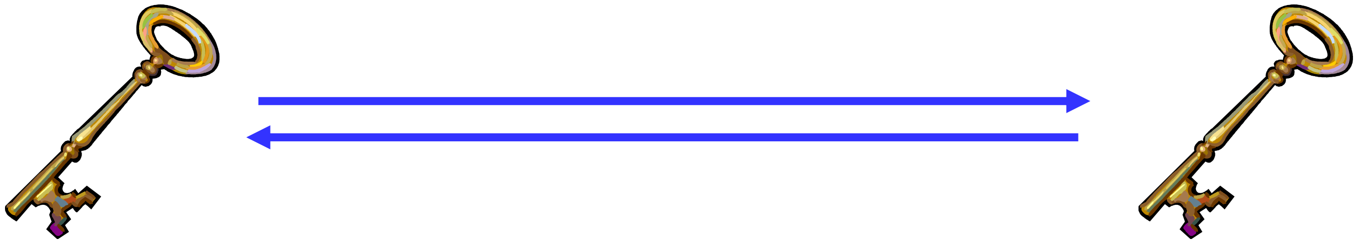
Rapelcgvba rkvfgf orpnhfr fbzrgvzrf
jr yvxr gb xrrc frpergf.

Encryption exists because sometimes
we like to keep secrets.

Cryptography is a mathematical function whereupon plaintext (“information in the clear”) is transmuted into a secret (“encrypted”) and can only be decrypted by someone who shares a common secret.

Symmetric keys
(Examples: DES, Triple-DES, AES)

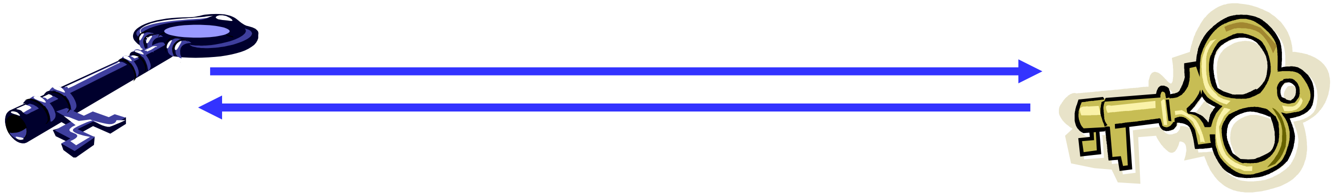
- A secret held in common by two parties
- Used to encrypt or decrypt a message in flight.
- Without the shared secret, a third party could not reasonably decrypt the message



- **The problem**: how does the secret key go from person A to person B?

Asymmetric keys
(Examples: Diffie-Hellman, RSA, DSA, Elliptic Curve)

- Corresponding secrets used to encrypt information
- Data encrypted by the private key can be encrypted by anyone with the public key
  - Only **Alice** has **Alice's** private key; if we can decrypt this message, it's from Alice.
  - If we encrypt the response with **Alice's** public key, only **Alice** will be able to read it.



- Mathematically more intensive than symmetric (and therefore much slower)
- **Question**: what if someone drops a bit? What happens to the message?

Hashing

(Examples: MD5, SHA-1, SHA-256, SHA-512, SHA-3)

- Computes a "message digest" based on a set of data
- Used to ensure data integrity
  - Checksum computation
  - Message Authentication Codes (MACs)
  - Makes sure your data is the same at the destination as it was at the source

What is a digital signature?

A mathematical algorithm used to validate both authenticity and integrity of content

Assure it hasn’t been modified

Assure it’s from a source you trust

Based on standard cryptographic algorithms used in the industry today

A **hash** component for integrity (SHA-2 most common)

An encryption of that hash with a **private key** (provides authenticity)

Verified by decrypting the hash with a **public key**, and then comparing that to a locally present hash

How digital signatures help

Hashing (a cryptographic checksum) provides integrity validation

One way function with no collisions

If you hash data twice, the result is always the same

If the data is modified by even one bit, result is (often wildly) different

Public-private key encryption provides authenticity

If you encrypt a string with a private key, anyone with the public key knows for certain it came from you

[Not a factor here, but] If you encrypt code with a public key, only the person with the private key can read it.

What don’t digital signatures do?

Prevent

Prevent access to images

- Your local access policies prevent this (this is RACF and similar)

Prevent

Prevent tampering after boot

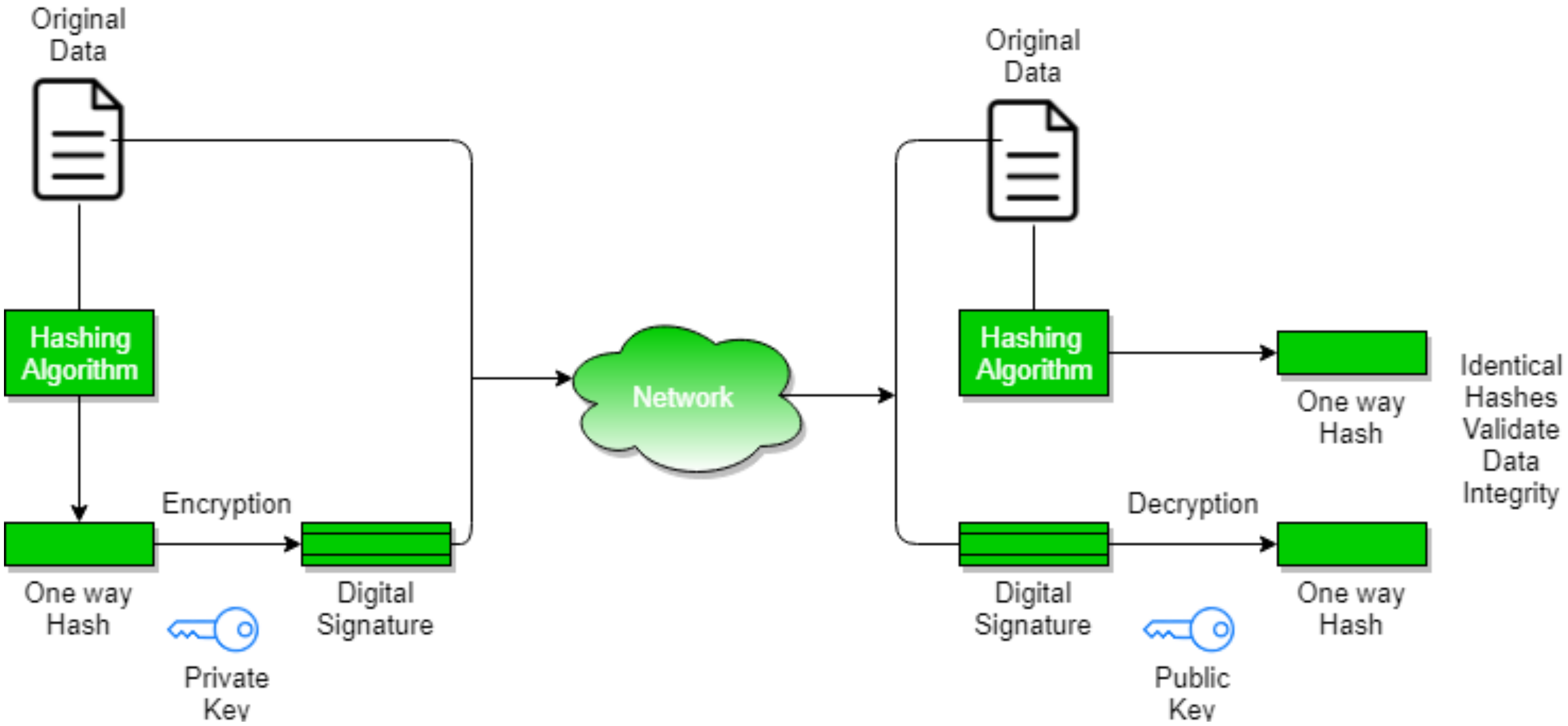
- Your local access policies prevent this
- Digital signature verification will prevent tampered code from booting, though

Prevent

Prevent authorized changes

- You do have to re-sign content after you update!
- Because you need a private key to do this, best to do this on a very secure system (in a clean room, if necessary)

What is a digital signature (picture version)



What is a digital signature (text version)

Source system (SYSTEMA)

If I hash a file (let’s call it **EXAMPLE.TXT**), it produces something like

0618451f 18c42ec6 19bb267e 989d35a1 ce42921d dbc6683c 35dd7ad9 ee2dee9c

If I encrypt that hash with Brian’s private key, it looks like

SKcxyiROK2iD6CQTS2py7+x4t3BB+bSC/QomG31Qdx0gJ7q4skMe0WiH5TmhA1s5MjoJwvKsXB3zCI2AXcipWBRm1G9YfbZLqXRM92Zcd5A4uUx66MHBjUsuR3QwoDbwAPdGxu6cqg27vSSBa51TgWQSktHX9JM8GZYceV0/ZxpFzx6cm0GvG4RDHr2MPz2DIHjg236f3f9j3YV1OE3j67U13VwkQdn/aZ07JTFyLCWIkZf+bYmwkkQ059sqHUNdZghEJEqVqbmy08MVIeb85gz0eMAgfeLmUKqW8xr5JyWdq9TEvmdrXFOvxRqM2HrtuxrtJ8tI/pawbZE/Y3LbSA==

We either append that signature to **EXAMPLE.TXT**, or give it its own file (**EXAMPLE.SIG**)

Let’s send the file and the signature to the destination system – let’s say we’re going to FTPS from SYSTEMA to SYSTEMB

Destination system (SYSTEMB)

If you hash **EXAMPLE.TXT** here, and it hasn’t been modified, same result

0618451f 18c42ec6 19bb267e 989d35a1 ce42921d dbc6683c 35dd7ad9 ee2dee9c

If you decrypt the signature on **EXAMPLE.TXT** with Brian’s public key,

SKcxyiROK2iD6CQTS2py7+x4t3BB+bSC/QomG31Qdx0gJ7q4skMe0WiH5TmhA1s5MjoJwvKsXB3zCI2AXcipWBRm1G9YfbZLqXRM92Zcd5A4uUx66MHBjUsuR3QwoDbwAPdGxu6cqg27vSSBa51TgWQSktHX9JM8GZYceV0/ZxpFzx6cm0GvG4RDHr2MPz2DIHjg236f3f9j3YV1OE3j67U13VwkQdn/aZ07JTFyLCWIkZf+bYmwkkQ059sqHUNdZghEJEqVqbmy08MVIeb85gz0eMAgfeLmUKqW8xr5JyWdq9TEvmdrXFOvxRqM2HrtuxrtJ8tI/pawbZE/Y3LbSA==

you get:

0618451f 18c42ec6 19bb267e 989d35a1 ce42921d dbc6683c 35dd7ad9 ee2dee9c

The hashes match!

You have a module which you **know** came from Brian, **and** no one’s messed with it.

How does this help with… service?

Recent ShopZ Changes

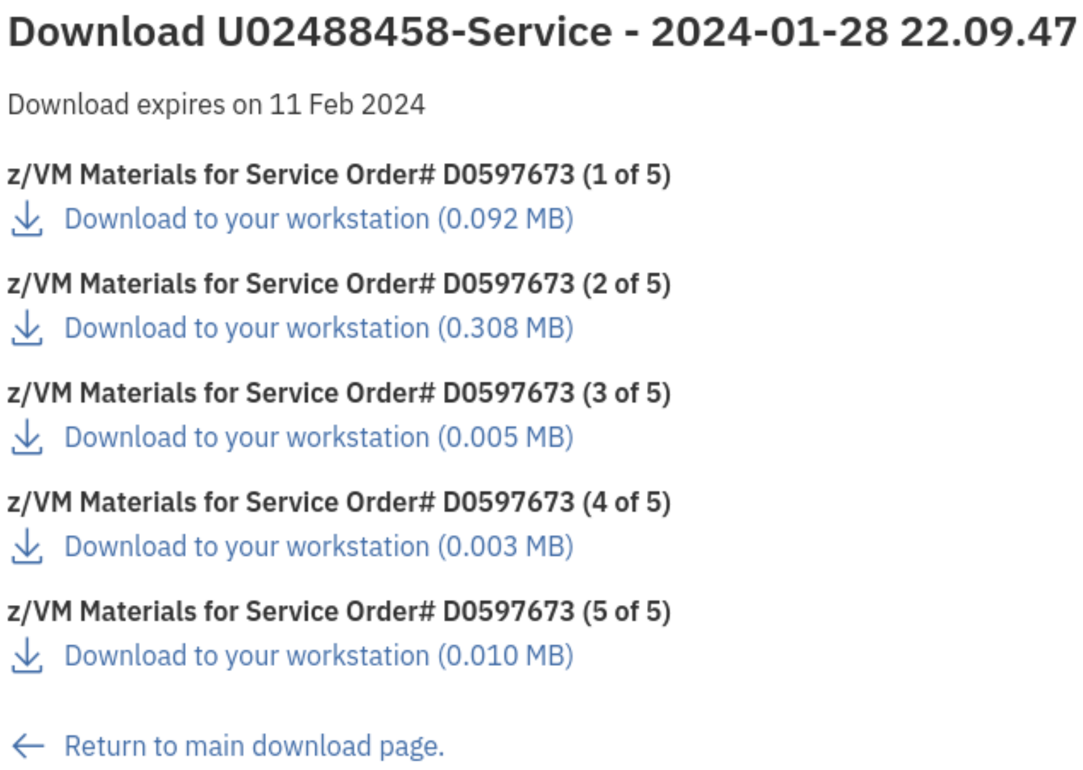
March 2024

- Extra cover letter provided with each order
  - More secure SHA256 hash values
  - Signed signature to authenticate the content
  - Certificates to warrant the signature

- For compatibility, old cover letter is still provided
  - Includes hash value to compare with e-mail

- In practice both cover letters are required
  - These are just a few small files

- Available from ShopZ since September 2023



Download U02488458-Service - 2024-01-28 22.09.47

Download expires on 11 Feb 2024

z/VM Materials for Service Order# D0597673 (1 of 5)
Download to your workstation (0.092 MB)

z/VM Materials for Service Order# D0597673 (2 of 5)
Download to your workstation (0.308 MB)

z/VM Materials for Service Order# D0597673 (3 of 5)
Download to your workstation (0.005 MB)

z/VM Materials for Service Order# D0597673 (4 of 5)
Download to your workstation (0.003 MB)

z/VM Materials for Service Order# D0597673 (5 of 5)
Download to your workstation (0.010 MB)

← Return to main download page.

GETSHOPZ – the preferred way to transfer service to z/VM

March 2024

Easy

Eliminates:

- Extra workstation tools to transfer files from the workstation to CMS
- Remembering the proper record format and setting that when uploading files
- Naming temporary files and find these back again later
- Extra utilities on CMS to unpack the files once uploaded to CMS
- Additional disk space to hold the temporary files before unpacking
- Authentication for file transfers to CMS
- Finding the hard-to-remember options like the TLS label by setting defaults
- Manually keeping a log file of service orders received

Secure

Complies with security policy:

- Data transfer secured with Transport Layer Security SSL)
- No password shared with workstation file transfer utilities
- Apply any security settings already defined in VM SSL
- Uses Digital Signature Validation to ensure authenticity of service package even when not using a direct connection
- Alerts users when using an expired service package

For clients with direct internet connection to download IBM service:

- Uses VM SSL and hostname validation to ensure service is only downloaded from the official IBM download site
- Ensures end-to-end integrity of the data

Quick

Makes transfer of service to z/VM quicker:

- Transfers multiple files in parallel to speed up the process on high-latency connections
- No temporary files to write and read to create SERVLINK files from downloaded service package
- Shows the order number and order signature on the web interface

For clients with direct internet connection to download IBM service:

- Avoids time consuming download to the workstation and upload to CMS
- Fewer steps by skipping the download and upload through the workstation

Flexible

Accommodate different client needs:

- Workstation upload with the same functionality for clients without direct internet connection
- Option to use a fixed web server port number for port-based firewalls
- Option to specify TCP/IP stack name for configurations with separate external stack
- Option to specify the hostname in the URL when TCP/IP configuration is not complete
- Support of token-based authentication for configurations with unique 3270 options
- Support to use proxy server for internet connectivity
- Ability to verify and extract service packages transferred to CMS with other tools (like IND$FILE, z/OS, or Linux)

GetShopz - Digital Signature Verification

March 2024

APAR VM66732 has closed - PTF UM90411 for z/VM 7.3 can now be ordered

Automatically verifies authenticity and integrity of the service received

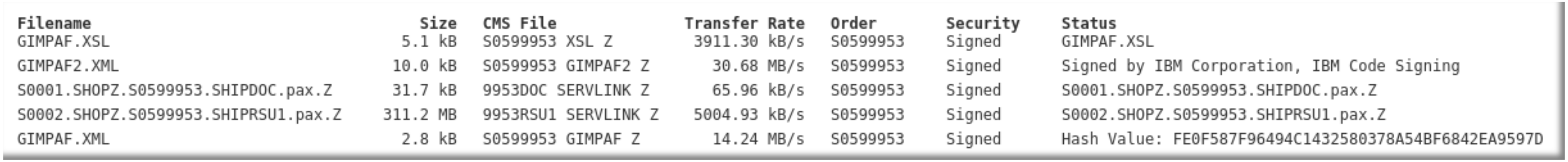
- Address Common Criteria requirement regarding “trusted update”
- Works for both “direct transfer” and “workstation upload”
- No SERVLINK files are retained without proof of authenticity

Additional function inspired by sponsor users and z/VM Council feedback

- Convenient log file of all received service packages with order hash value
- New ISOLATED option for workstations without internet connectivity
- New EXTRACT function for clients without browser access to their z/VM system
- Suggested browser extension to copy and paste the five Shopz URLs at once

Web Application Status Display

March 2024



```
Filename                               Size  CMS File              Transfer Rate  Order        Security    Status
GIMPAF.XSL                           5.1 kB  S0599953 XSL Z         3911.30 kB/s  S0599953     Signed      GIMPAF.XSL
GIMPAF2.XML                         10.0 kB  S0599953 GIMPAF2 Z       30.68 MB/s  S0599953     Signed      Signed by IBM Corporation, IBM Code Signing
S0001.SHOPZ.S0599953.SHIPDOC.pax.Z  31.7 kB  9953DOC SERVLINK Z       65.96 kB/s  S0599953     Signed      S0001.SHOPZ.S0599953.SHIPDOC.pax.Z
S0002.SHOPZ.S0599953.SHIPRSU1.pax.Z 311.2 MB  9953RSU1 SERVLINK Z   5004.93 kB/s  S0599953     Signed      S0002.SHOPZ.S0599953.SHIPRSU1.pax.Z
GIMPAF.XML                           2.8 kB  S0599953 GIMPAF Z        14.24 MB/s  S0599953     Signed      Hash Value: FE0F587F96494C1432580378A54BF6842EA9597D
```

Filename

- Shows transfer or upload name
- Progress bar as blue line
- Now used to identify contents of new GIMZIP (v7) packages

Size

- Compressed file as transferred

CMS File

- File on CMS after unpacking
- Larger than transfer (~ 2x)
- Determined after transfer when cover letter has been received

Transfer Rate

- Average final throughput rate
- Data received (in progress)

Order

- Order number from Shopz
- Note: Prefix letter will vary

Security

- **Signed**: verified signature
- **IBM-SSL**: direct transfer IBM
- **SSL**: transfer from elsewhere
- **Proxy**: transfer through proxy
- **Hash**: verified only hash value

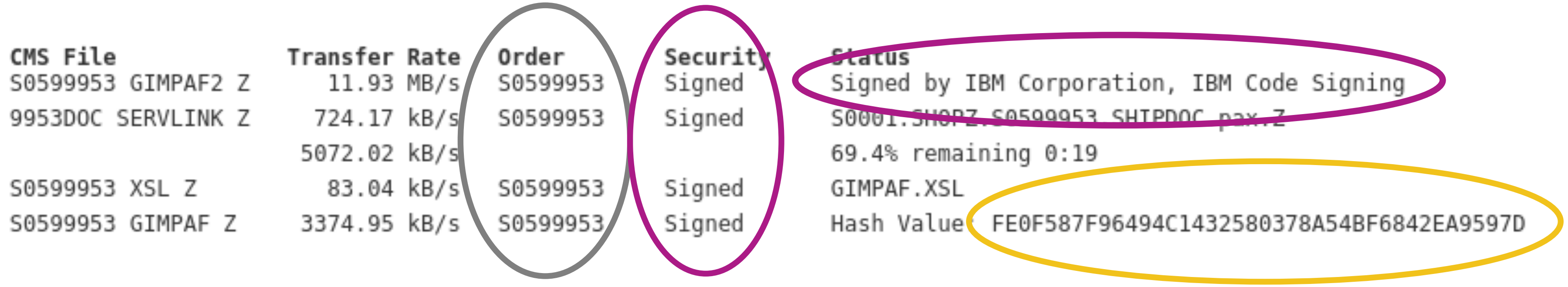
Status

- Percentage complete and expected time remaining
- Signature authority for signed cover letter
- Hash value for GIMPAF file
- Original file name

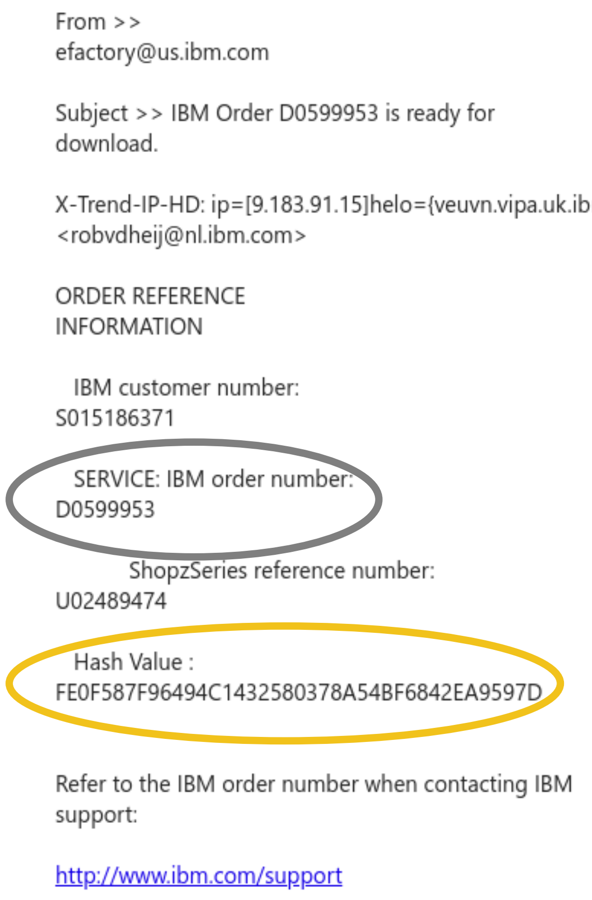
Recognize a Service Order

Web Application

March 2024



```
CMS File             Transfer Rate  Order      Security  Status
S0599953 GIMPAF2 Z      11.93 MB/s  S0599953   Signed    Signed by IBM Corporation, IBM Code Signing
9953DOC SERVLINK Z     724.17 kB/s  S0599953   Signed    S0001.SHOPZ.S0599953.SHIPDOC.pax.Z
                      5072.02 kB/s                       69.4% remaining 0:19
S0599953 XSL Z          83.04 kB/s  S0599953   Signed    GIMPAF.XSL
S0599953 GIMPAF Z     3374.95 kB/s  S0599953   Signed    Hash Value: FE0F587F96494C1432580378A54BF6842EA9597D
```



From >>
efactory@us.ibm.com

Subject >> IBM Order D0599953 is ready for download.

X-Trend-IP-HD: ip=[9.183.91.15]helo={veuvn.vipa.uk.ibm.com}sender=(efactory@us.ibm.com)recipient=<robvdheij@nl.ibm.com>

ORDER REFERENCE
INFORMATION

IBM customer number:
S015186371

SERVICE: IBM order number:
D0599953

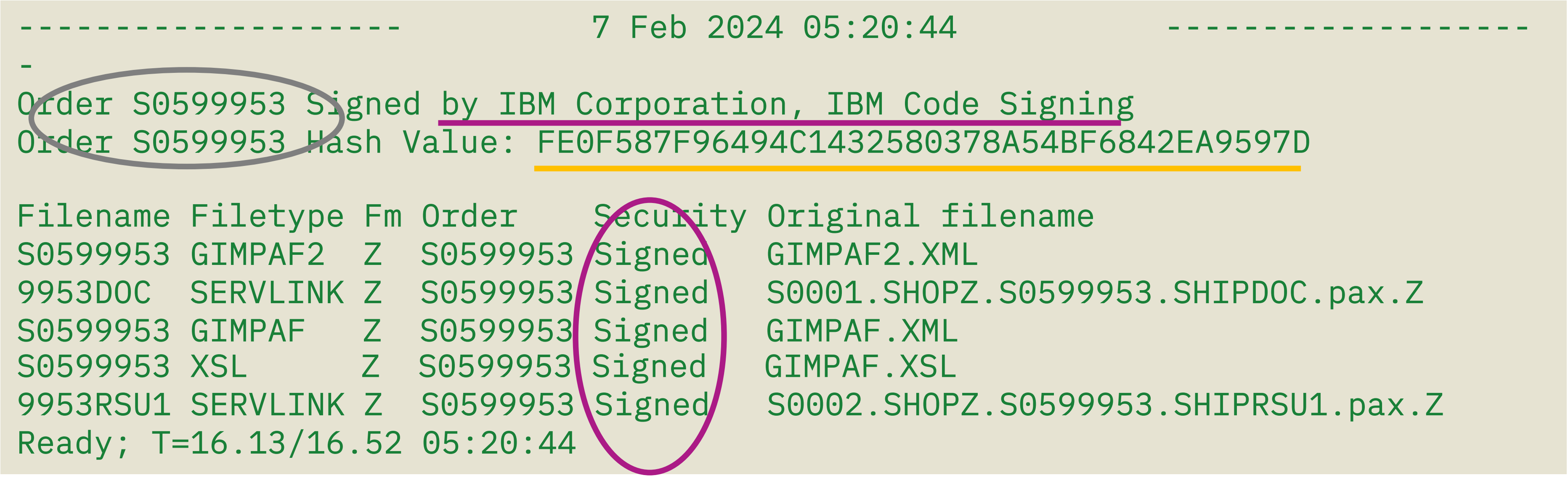
ShopzSeries reference number:
U02489474

Hash Value :
FE0F587F96494C1432580378A54BF6842EA9597D

Refer to the IBM order number when contacting IBM support:

http://www.ibm.com/support

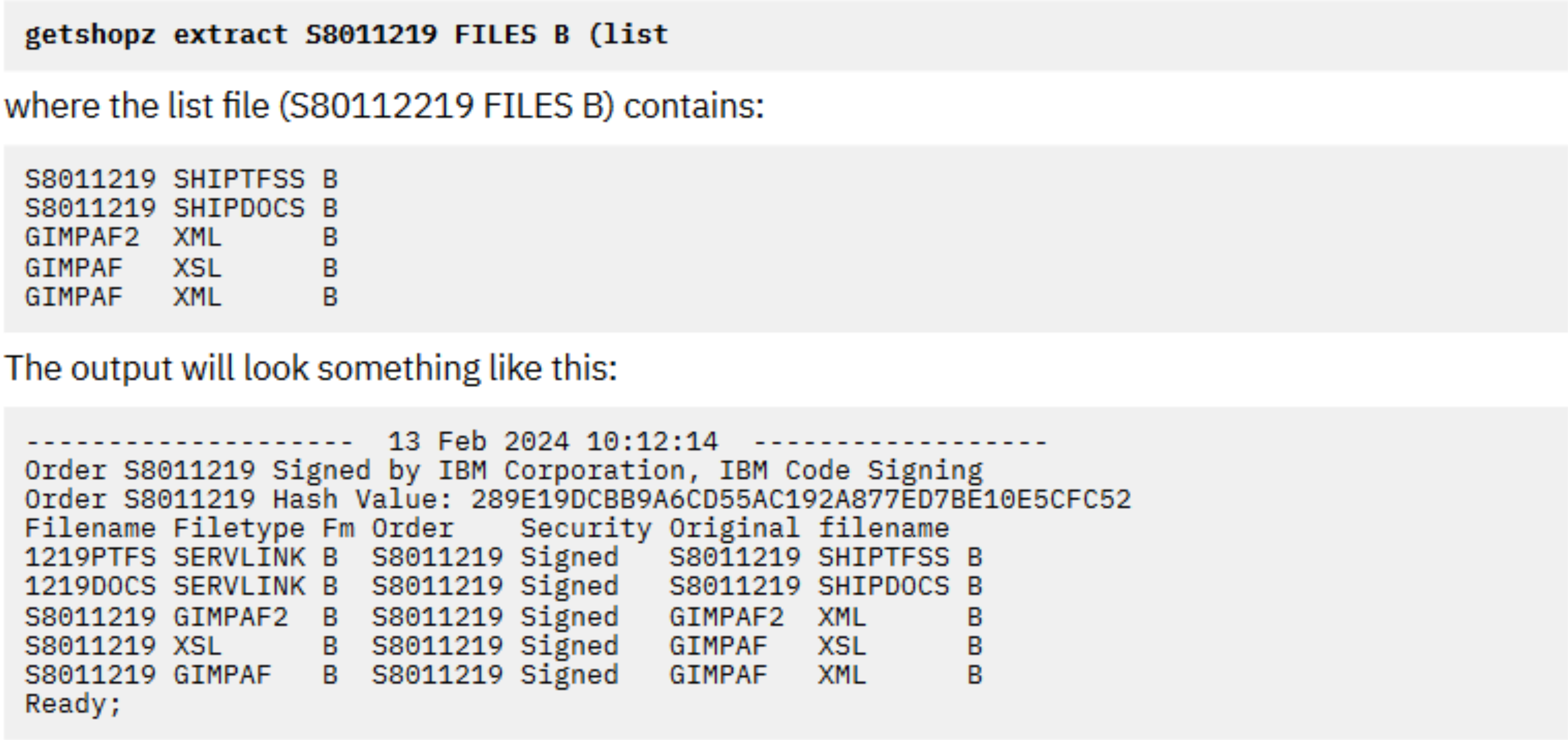
CMS Session and Log File



```
--------------------          7 Feb 2024 05:20:44          --------------------
-
Order S0599953 Signed by IBM Corporation, IBM Code Signing
Order S0599953 Hash Value: FE0F587F96494C1432580378A54BF6842EA9597D

Filename Filetype Fm Order    Security Original filename
S0599953 GIMPAF2  Z  S0599953 Signed   GIMPAF2.XML
9953DOC  SERVLINK Z  S0599953 Signed   S0001.SHOPZ.S0599953.SHIPDOC.pax.Z
S0599953 GIMPAF   Z  S0599953 Signed   GIMPAF.XML
S0599953 XSL      Z  S0599953 Signed   GIMPAF.XSL
9953RSU1 SERVLINK Z  S0599953 Signed   S0002.SHOPZ.S0599953.SHIPRSU1.pax.Z
Ready; T=16.13/16.52 05:20:44
```

Extract and verify previously uploaded package



```
getshopz extract S8011219 FILES B (list
```

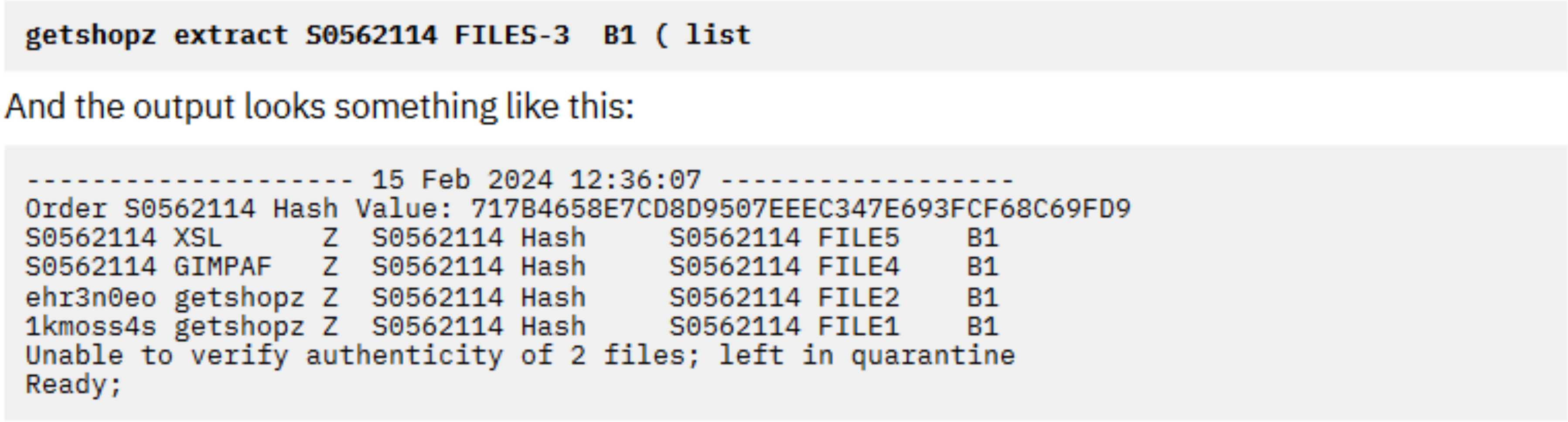
where the list file (S80112219 FILES B) contains:

```
S8011219 SHIPTFSS B
S8011219 SHIPDOCS B
GIMPAF2  XML      B
GIMPAF   XSL      B
GIMPAF   XML      B
```

The output will look something like this:

```
--------------------  13 Feb 2024 10:12:14  ------------------
Order S8011219 Signed by IBM Corporation, IBM Code Signing
Order S8011219 Hash Value: 289E19DCBB9A6CD55AC192A877ED7BE10E5CFC52
Filename Filetype Fm Order    Security Original filename
1219PTFS SERVLINK B  S8011219 Signed   S8011219 SHIPTFSS B
1219DOCS SERVLINK B  S8011219 Signed   S8011219 SHIPDOCS B
S8011219 GIMPAF2  B  S8011219 Signed   GIMPAF2  XML      B
S8011219 XSL      B  S8011219 Signed   GIMPAF   XSL      B
S8011219 GIMPAF   B  S8011219 Signed   GIMPAF   XML      B
Ready;
```

GetShopz Quarantine of Files

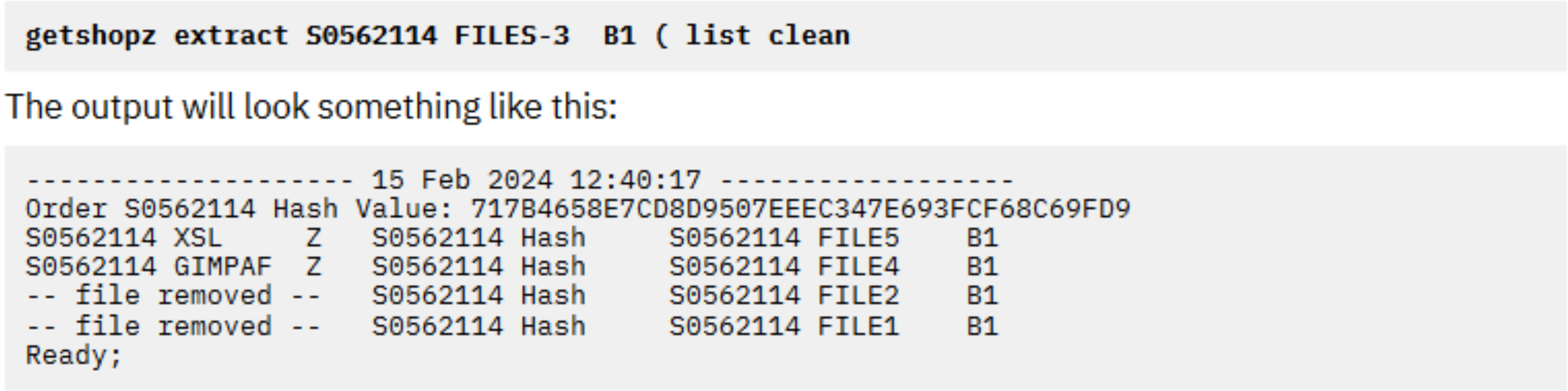


```
getshopz extract S0562114 FILES-3  B1 ( list
```

And the output looks something like this:

```
-------------------- 15 Feb 2024 12:36:07 ------------------
Order S0562114 Hash Value: 717B4658E7CD8D9507EEEC347E693FCF68C69FD9
S0562114 XSL      Z  S0562114 Hash     S0562114 FILE5    B1
S0562114 GIMPAF   Z  S0562114 Hash     S0562114 FILE4    B1
ehr3n0eo getshopz Z  S0562114 Hash     S0562114 FILE2    B1
1kmoss4s getshopz Z  S0562114 Hash     S0562114 FILE1    B1
Unable to verify authenticity of 2 files; left in quarantine
Ready;
```

Quarantined files cannot be worked with in CMS.
- Use FILELIST MIXEDON option or the CLEAN option of GetShopz



```
getshopz extract S0562114 FILES-3  B1 ( list clean
```

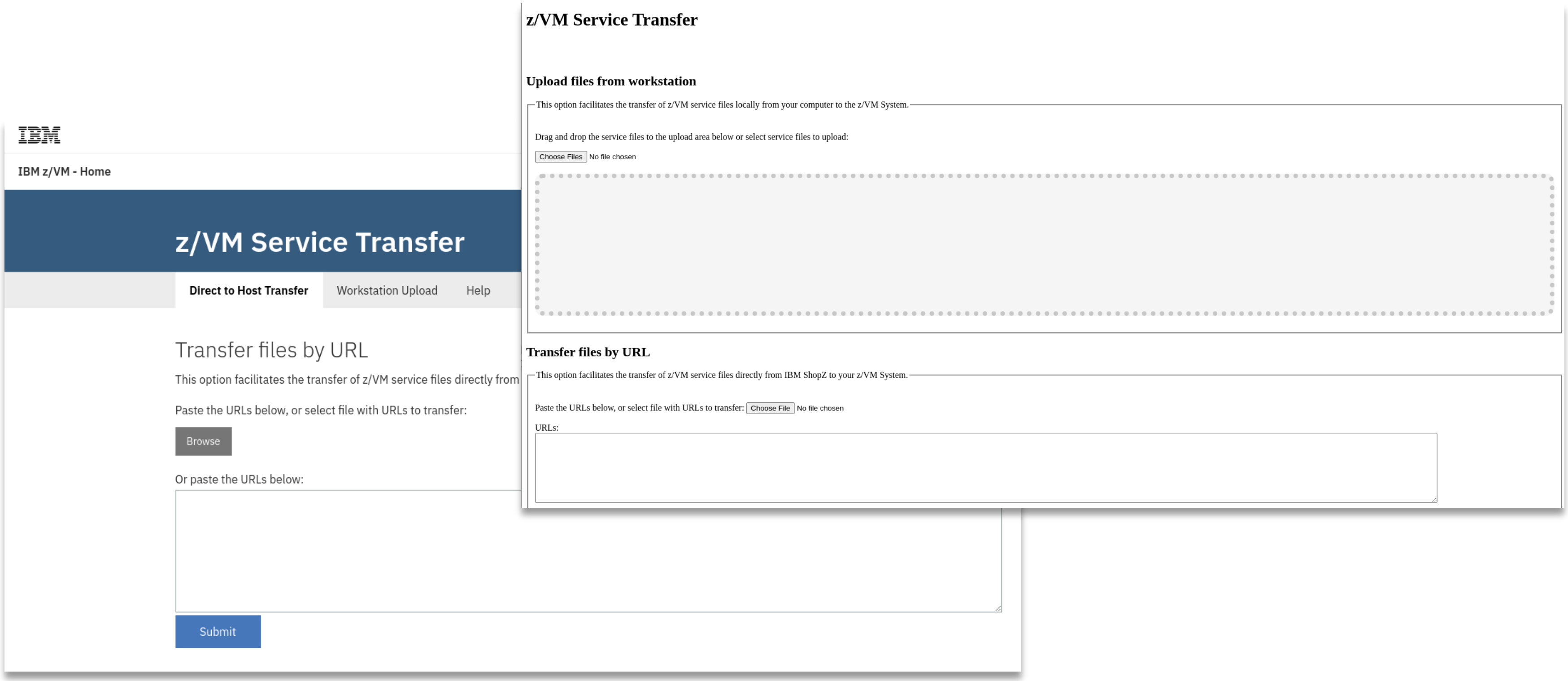
The output will look something like this:

```
-------------------- 15 Feb 2024 12:40:17 ------------------
Order S0562114 Hash Value: 717B4658E7CD8D9507EEEC347E693FCF68C69FD9
S0562114 XSL     Z   S0562114 Hash     S0562114 FILE5    B1
S0562114 GIMPAF  Z   S0562114 Hash     S0562114 FILE4    B1
-- file removed --   S0562114 Hash     S0562114 FILE2    B1
-- file removed --   S0562114 Hash     S0562114 FILE1    B1
Ready;
```

Workstation Without Internet Connectivity

March 2024

- New ISOLATED option to use only built-in web resources



z/VM Service Transfer

Transfer files by URL

This option facilitates the transfer of z/VM service files directly from

Paste the URLs below, or select file with URLs to transfer:

Or paste the URLs below:

z/VM Service Transfer

Upload files from workstation

This option facilitates the transfer of z/VM service files locally from your computer to the z/VM System.

Drag and drop the service files to the upload area below or select service files to upload:

No file chosen

Transfer files by URL

This option facilitates the transfer of z/VM service files directly from IBM ShopZ to your z/VM System.

Paste the URLs below, or select file with URLs to transfer: No file chosen

URLs:

Summary

March 2024

- Cover letters must be included to produce SERVLINK files used to apply service

- Digital signature means that we can **verify integrity and authenticity** even when service files were delivered via an untrusted route

- For clients without web browser connection with workstation, the **EXTRACT** function of GETSHOPZ provides the same verification when using other data transfer tools

- **Logging of received service and cover letters** is provided

How does this help with… guests?

Secure IPL for z/VM Guests

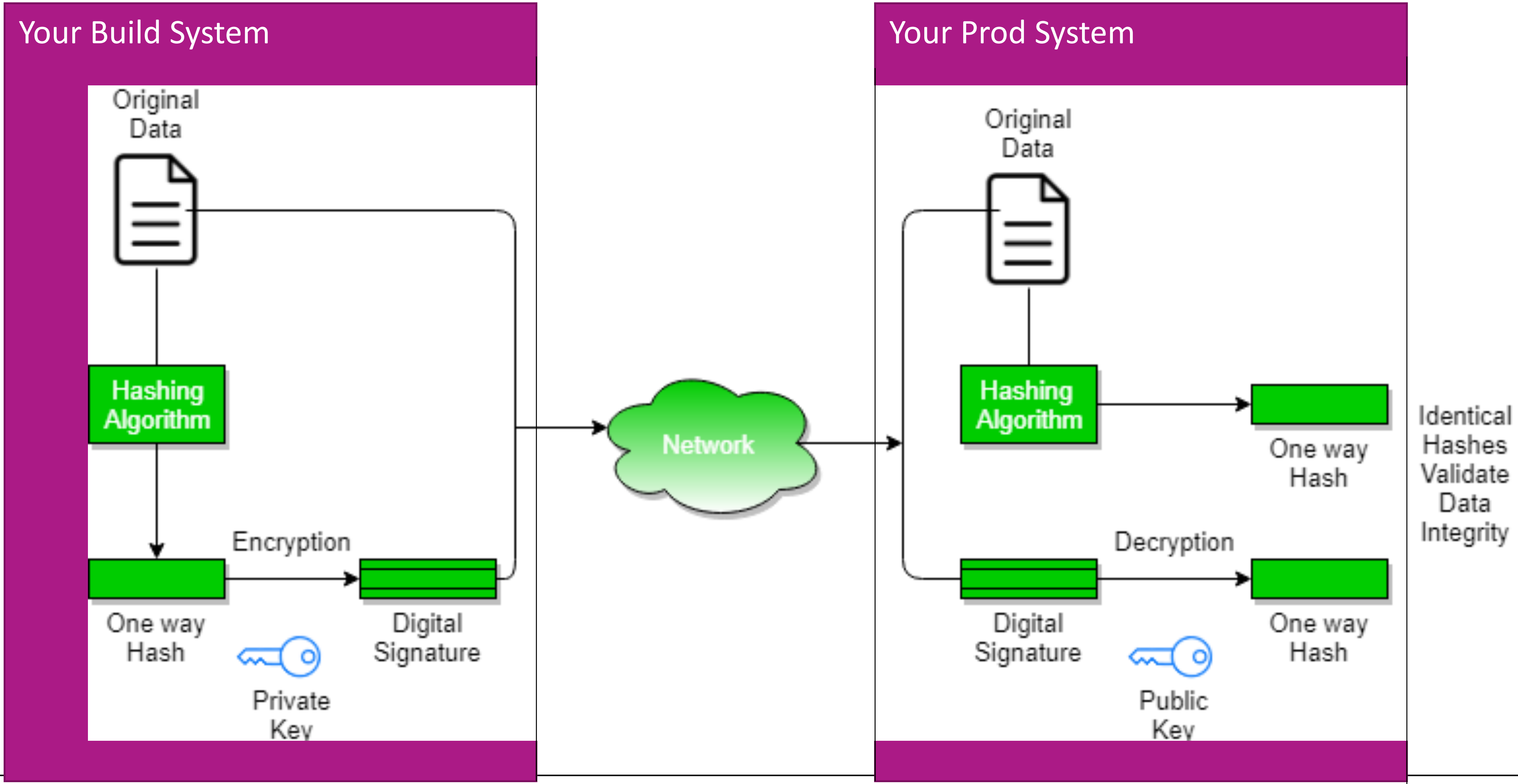
June 2023

- **Assures that the content an administrator boots is unmodified from time of install**

- **New supply-chain requirement for a lot of industry regulations**

- **z/VM provides support for secure boot of guest operating systems**
  - Support added when IPL’ing from ECKD or from SCSI storage (DASD)
  - A guest must IPL LOADDEV, not IPL *vdev*
  - A securely IPL’d guest will behave the same way as a guest booted in its own partition

What is a digital signature (picture version)



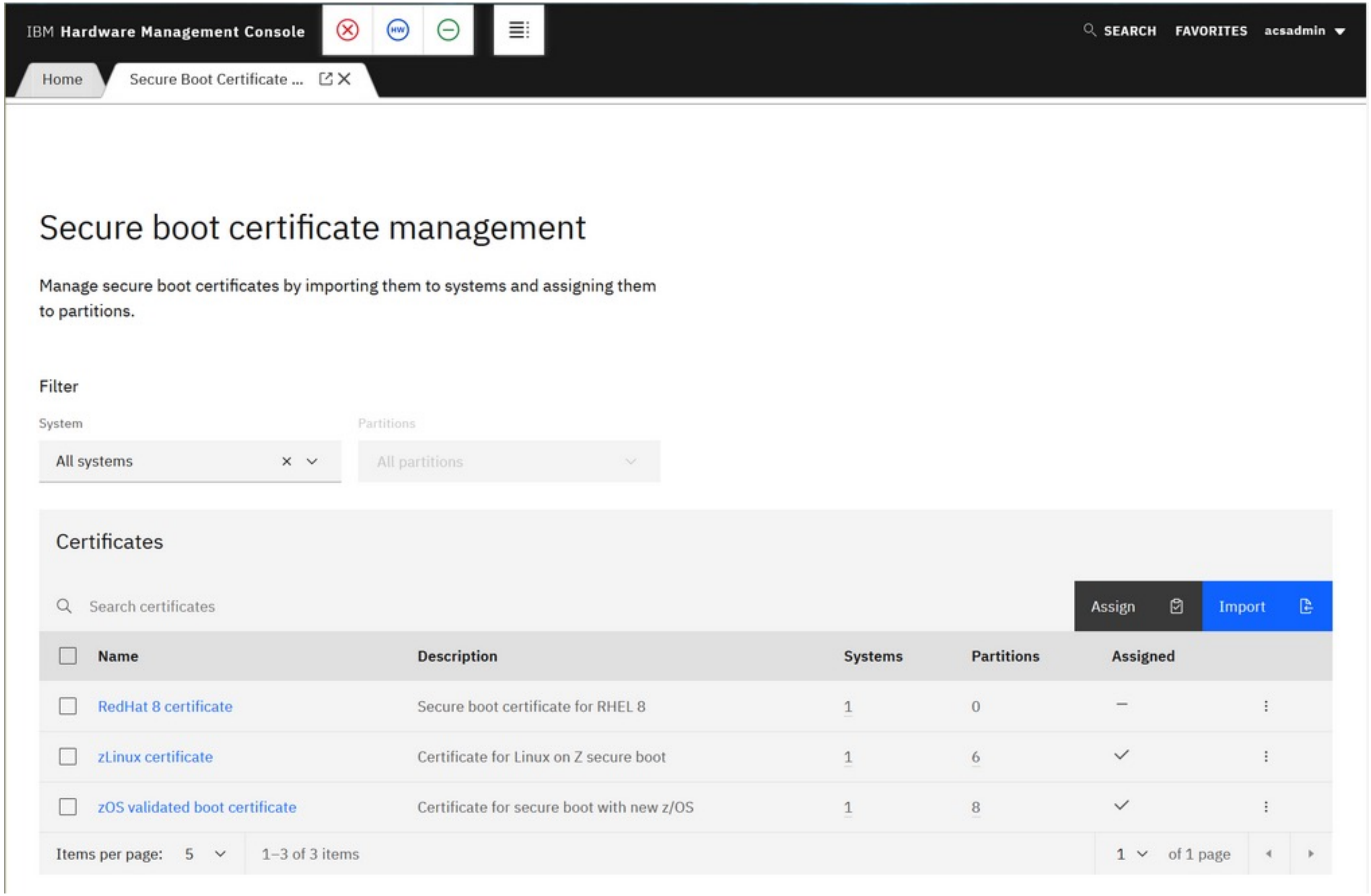
Secure IPL for z/VM Guests

June 2023

How to use Secure IPL

- Upgrade machine firmware on your IBM z16 or IBM LinuxONE Emperor 4
  - Driver D51C bundle 19
- Install the levels of software required for support
  - z/VM PTFs as specified
  - z/OS PTFs as specified
  - Linux updates -- more support required than what was previously available for secure boot in an LPAR
- Import necessary certificate(s) with **public** key(s) into the HMC certificate store
  - Public key **(.p7b format)** must match signing private key
  - Check with your vendor(s) for more details
- Assign them to the LPARs where the guest will run
  - Any guest capable of, and attempting to, secure boot will use these certificates
- Use **SET LOADDEV** command to set load parameters
- **IPL LOADDEV** to boot your secure guest

SE/HMC Certificate Management – Certificate View



Secure boot certificate management

Manage secure boot certificates by importing them to systems and assigning them to partitions.

Filter

System

All systems

Partitions

All partitions

Certificates

Search certificates

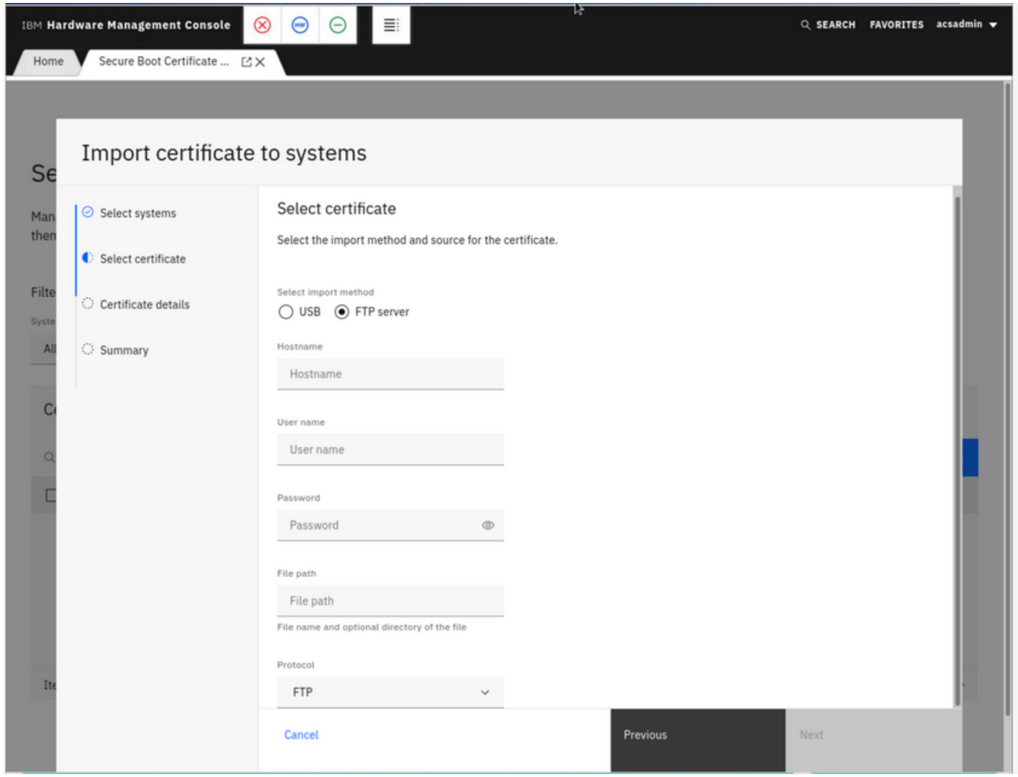
Assign Import

□	Name	Description	Systems	Partitions	Assigned
□	RedHat 8 certificate	Secure boot certificate for RHEL 8	1	0	–
□	zLinux certificate	Certificate for Linux on Z secure boot	1	6	✓
□	zOS validated boot certificate	Certificate for secure boot with new z/OS	1	8	✓

Items per page: 5   1–3 of 3 items   1 of 1 page

#vmworkshop

SE/HMC Certificate Management - Import



Import certificate to systems

- Select systems
- Select certificate
- Certificate details
- Summary

Select certificate

Select the import method and source for the certificate.

Select import method
○ USB ● FTP server

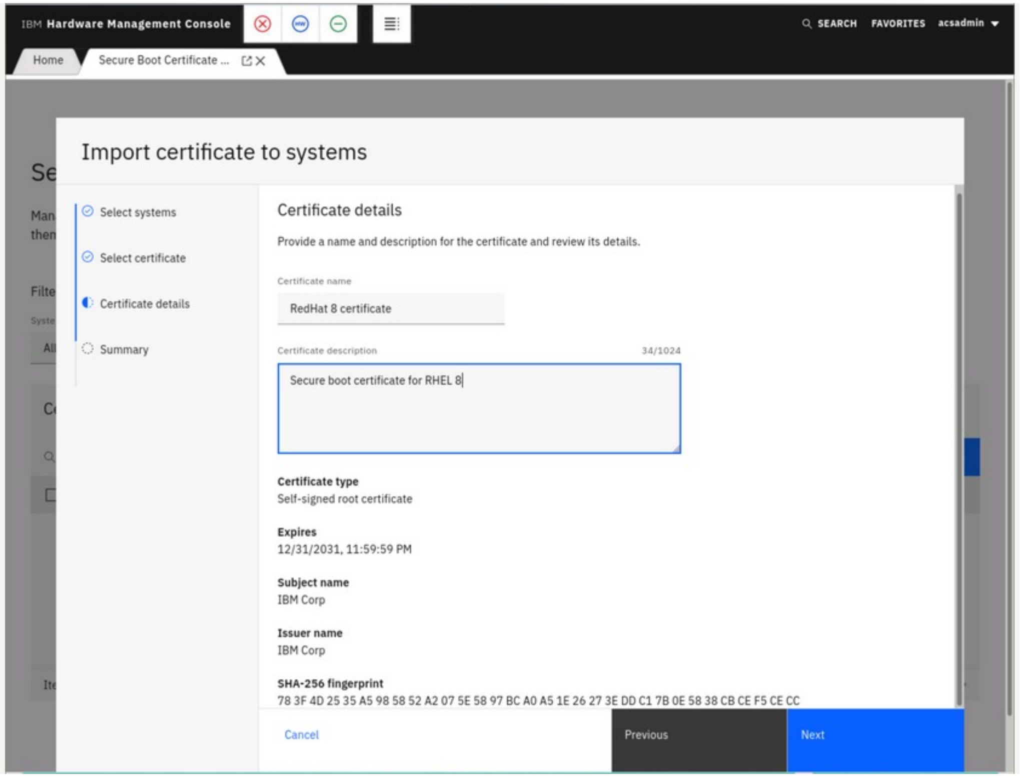
Hostname: Hostname

User name: User name

Password: Password

File path: File path
File name and optional directory of the file

Protocol: FTP



Import certificate to systems

- Select systems
- Select certificate
- Certificate details
- Summary

Certificate details

Provide a name and description for the certificate and review its details.

Certificate name: RedHat 8 certificate

Certificate description (34/1024): Secure boot certificate for RHEL 8

Certificate type
Self-signed root certificate

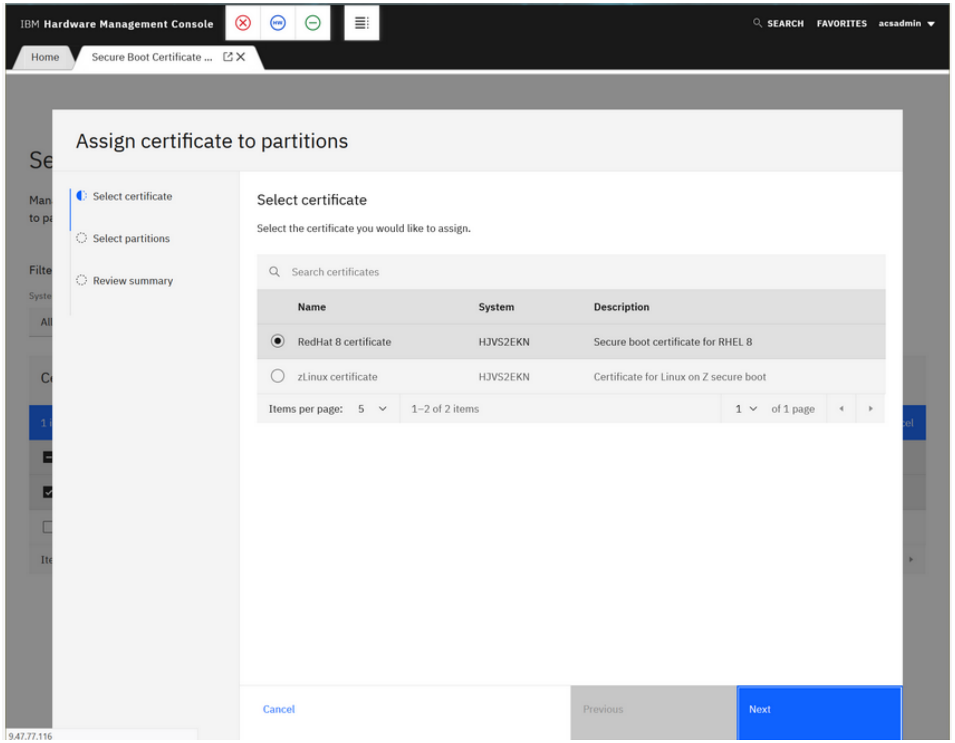
Expires
12/31/2031, 11:59:59 PM

Subject name
IBM Corp

Issuer name
IBM Corp

SHA-256 fingerprint
78 3F 4D 25 35 A5 98 58 52 A2 07 5E 58 97 BC A0 A5 1E 26 27 3E DD C1 7B 0E 58 38 CB CE F5 CE CC

SE/HMC Certificate Management - Assign



Assign certificate to partitions

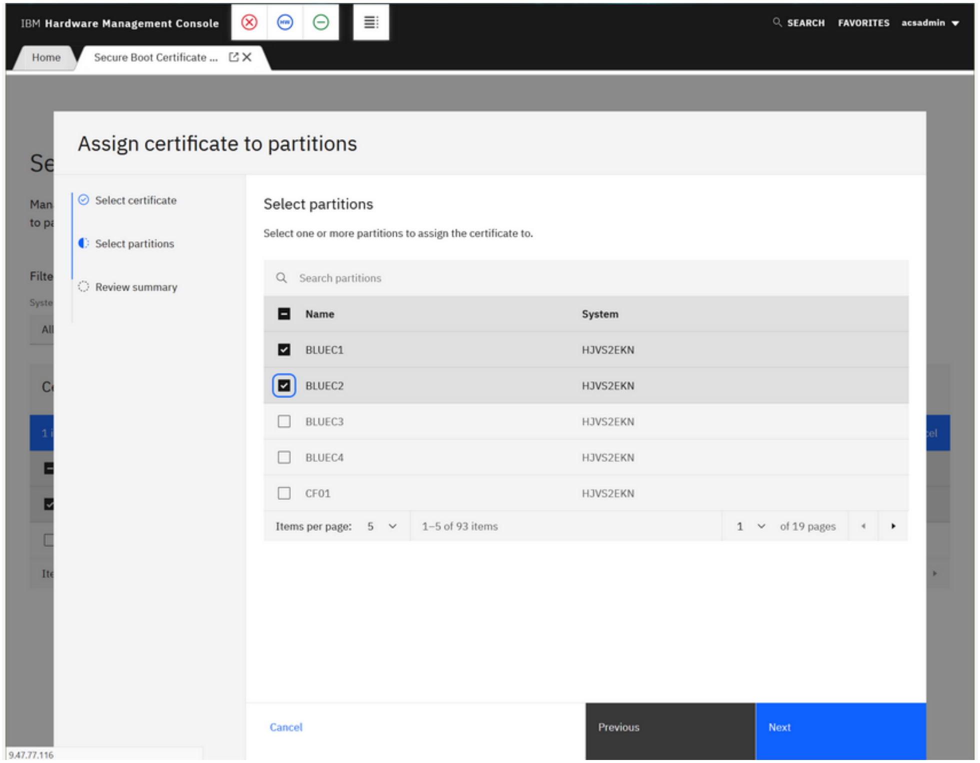
Select certificate

Select the certificate you would like to assign.

Search certificates

	Name	System	Description
●	RedHat 8 certificate	HJVS2EKN	Secure boot certificate for RHEL 8
○	zLinux certificate	HJVS2EKN	Certificate for Linux on Z secure boot

Items per page: 5 1–2 of 2 items 1 of 1 page



Assign certificate to partitions

Select partitions

Select one or more partitions to assign the certificate to.

Search partitions

	Name	System
☑	BLUEC1	HJVS2EKN
☑	BLUEC2	HJVS2EKN
□	BLUEC3	HJVS2EKN
□	BLUEC4	HJVS2EKN
□	CF01	HJVS2EKN

Items per page: 5 1–5 of 93 items 1 of 19 pages

#vmworkshop

SET LOADDEV SCSI (Class G)

June 2023

```
>>-Set--LOADDEV-+--CLEAR-----------------------------------+-><
                |            +-SCSI-+                      |
                +-+-------+-++------+-| SCSI Operands |--+-+
                  '-CLEAR-' '                            '
                            '--ECKD---| ECKD Operands |--'

SCSI operands
   .----------------------------------------------.
   V                                              |
|----+-DEVice--fcp_vdev-------------------------+-+----------|
     +-PORTname--hhhhhhhh hhhhhhhh--------------+
     +-LUN--hhhhhhhh hhhhhhhh-------------------+
     +-BOOTprog--+--bootprog_number-+-----------+
     |           '--AUTOmatic-------'           |
     |                                          |
     +-BR_LBA--hhhhhhhh hhhhhhhh----------------+
     +-+-NOSECURE-+-----------------------------+
     | '-SECURE---’                             |
     |          .-APPend-.                      |
     '-SCPdata--+--------+--+-----+--+-'text'-+-'
                +-NEW----+  '-HEX-'  '-text---'
                '-offset-'
```

- SECURE valid only when DEVice operand is used
- LOADDEV directory statement updated accordingly
- DUMPDEV has similar enhancements
- Associated DIRMAINT support added (VM66424)

SET LOADDEV ECKD (Class G)

June 2023

```
>>-Set--LOADDEV-+--CLEAR-----------------------------------+-><
                |            +-SCSI-+                      |
                +-+-------+-++------+-| SCSI Operands |--+-+
                  '-CLEAR-' '                            '
                            '--ECKD---| ECKD Operands |--'

ECKD operands
    .----------------------------------------------.
   V                                              |
|----+-DEVice--eckd_vdev------------------------+-+----------|
     |                                          |
     +-BOOTprog--+-bootprog_number--+-----------+
     |           '--AUTOmatic-------'           |
     |                                          |
     +-BOOTREC-+-cyl head rec--+----------------+
     |         '--LABEL--------'                |
     |                                          |
     +-+-NOSECURE-+-----------------------------+
     | '-SECURE---’                             |
     |          .-APPend-.                      |
     '-SCPdata--+--------+--+-----+--+-'text'-+-'
                +-NEW----+  '-HEX-'  '-text---'
                '-offset-'
```

- SECURE valid only when DEVice operand is used
- LOADDEV directory statement updated accordingly
- DUMPDEV has similar enhancements
- Associated DIRMAINT support added (VM66424)

IPL LOADDEV / DUMPDEV (Class G)

June 2023

```
>>-+-Ipl--+-+-system_name---------------+--| Parameters |----------+-+-
   |      | '-vdev--| Device Operands |-'                          | |
   |      |                                                        | |
   |      '--+--fcp_vdev--+-------------------+-| LDIPL Operands |-' |
   |         |            '-DUMP--+---------+-'                      |
   |         |                    '-NSSDATA-' |                      |
   |         '--LOADDEV-----------------------'                      |
   |         |                                |                      |
   |         '--DUMPDEV-----------------------'                      |
   '-IPL-------------------------------------------------------------'

LDIPL Operands
|--+---------------------+--+------+---+------+-----------------|
   '-LOADParm--load_parm-'  '-STOP-'   '-ATTN-'
```

- LOADDEV / DUMPDEV point to parms set with SET LOADDEV or DUMPDEV
- IPL directory statement contains new LOADDEV option
- OPTION directory statement can enforce use with SECUREIPLREQ

Secure IPL for z/VM Guests

June 2023

- **Available for z/VM V7.3**
  - https://www.vm.ibm.com/newfunction/#gsipl
  - Requires Driver D51C Bundle 19 for IBM z16 or IBM LinuxONE Emperor 4
  - Refer to Machine Field Alert for required Linux OS services levels
    - https://www-40.ibm.com/servers/resourcelink/lib03020.nsf/pagesByDocid/272B3DD994A65B538525899F005FA0E6?OpenDocument

- z/OS will only run in audit-mode, due to a requirement for Virtual Flash Memory
  - Use SET LOADDEV…NOSECURE when IPL'ing z/OS guests under z/VM

Component	APAR	PTF	RSU
CP	VM66434	UM90281	RSU2302
DirMaint	VM66424	UV99435	RSU2302
SMAPI	VM66650	UM90300	RSU2302

How does this help with… the future?

z/VM Security Certifications

z/VM releases not listed are "designed to conform to the standards of each security evaluation."

z/VM Level	Common Criteria	
z/VM 7.4	*Announced – coming in ~3Q2024*	
z/VM 7.3	*Not evaluated ("designed to conform to standards")*	
z/VM 7.2	***BSI OSPP (with Virt and Labeled Security extensions) at EAL 4+ – Completed!***	***NIAP VPP with Server Virt. Extended Package – Completed!***
z/VM 7.1	*Not evaluated ("designed to conform to standards")*	
z/VM 6.4	OSPP with Labeled Security and Virtualization at EAL 4+ -- ***COMPLETED!*** *http://www.ocsi.isticom.it/index.php/elenchi-certificazioni/in-corso-di-valutazione*	

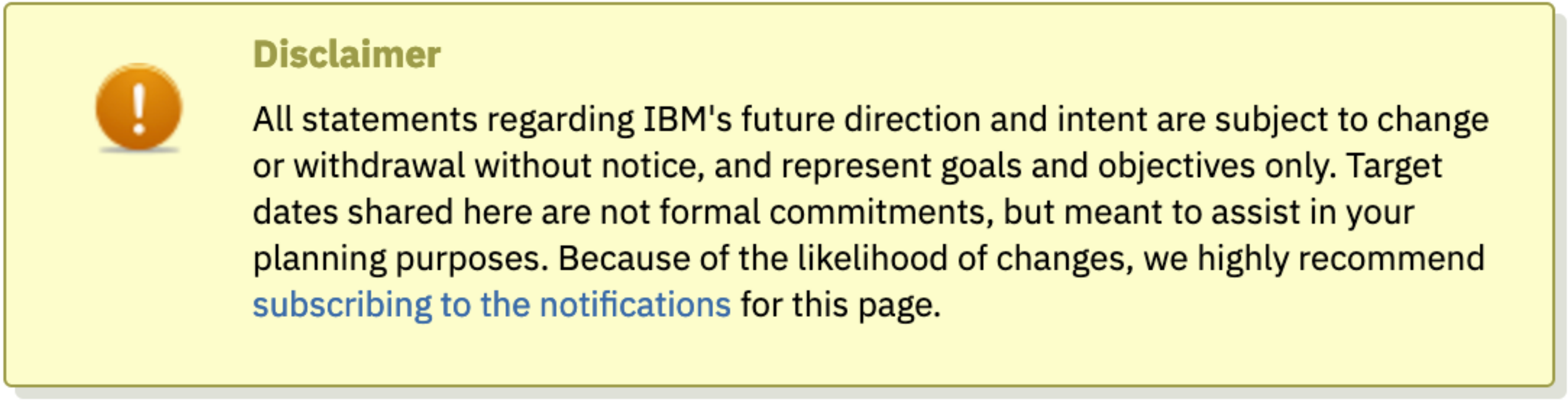
z/VM Level	FIPS 140-n
z/VM 7.4	*Announced – coming in 3Q2024*
z/VM 7.3	*Not evaluated ("designed to conform to standards")*
z/VM 7.2	***FIPS 140-2 L1 for z/VM System SSL and ICSFLIB – Completed!***
z/VM 7.1	*Not evaluated ("designed to conform to standards")*
z/VM 6.4	FIPS 140-2 L1 – ***COMPLETED!*** *https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3374*

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

This slide intentionally left blank.

- *Wow, I’m glad the Workshop isn’t recording this session.*

This slide (also) intentionally left blank.



Disclaimer

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Target dates shared here are not formal commitments, but meant to assist in your planning purposes. Because of the likelihood of changes, we highly recommend subscribing to the notifications for this page.

https://www.vm.ibm.com/newfunction

Summary

Summary

- You need to assure that the code you're installing… the code you're IPL'ing... is the code you intended

- Service now allows for validation of content via ShopZ and the z/VM GETSHOPZ utility
  - RSA2048/SHA256, signed by IBM
  - Matches what happens on z/OS
  - In place today

- Guests can be validated in terms of the operating system you're loading
  - Linux or z/OS
  - …on an IBM z16 or LinuxONE 4 machine
  - …with appropriate public keys installed on the SE
  - Available today

- This sort of assurance will only grow over time
  - Keep an eye on the rules and regulations to which you must adhere
  - Keep an eye on the VM Council and the z/VM New Function webpage
    - https://www.vm.ibm.com/newfunction/

For more information…

Brian W. Hugenbruch
IBM LinuxONE Resiliency Lead &&
IBM z/VM Security and Cryptography Lead

- **IBM webpage**:
  https://www.vm.ibm.com/devpages/hugenbru/

- **Technical blog**: https://bwhugen.github.io

Social Media:

https://www.linkedin.com/in/bwhugen/

@the_lettersea

@apictureofaman@infosec.exchange

Arielle Goldberg
IBM z/VM Software Developer

https://www.linkedin.com/in/ariellemgoldberg

THANK YOU