

z/OS 3.1 IBM Education Assistant

Solution Name: ICSF Clear Key Health Check

Solution Element(s): ICSF

July 2023



Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

- See url <http://www.ibm.com/legal/copytrade.shtml> for a list of trademarks.
- Additional Trademarks:
 - None

Objectives

- New ICSF health check lists the labels of keys that are unencrypted

Overview

- Who (Audience)
 - System Administrators
- What (Solution)
 - Clear Key Health Check
- Wow (Benefit / Value, Need Addressed)
 - Lists keys in the CKDS, PKDS, and TKDS that are not encrypted and allows the system admin to make informed decisions about which keys to use

Usage & Invocation

- Callable service CSFKDSL can be used to list clear key labels
- New search criteria added to KDSL
 - X'0008' can be specified in the search_criteria parameter to filter for clear keys
 - Applicable for CKDS, PKDS, and TKDS
- KDSL outputs a list of clear key labels found in the active KDS if LABELS is specified as the output format

Usage & Invocation (cont.)

- Clear key health check will be registered upon initialization of ICSF
- This health check will issue a message in the job log that states whether there are clear keys found in the KDS
 - CSFH0055I: No clear keys were found in the CKDS, PKDS, or TKDS.
 - CSFH0056E: Clear keys in the CKDS, PKDS, or TKDS were found.
- If any clear keys are found, a list of clear key labels for each active KDS can be found in the health check job log

Usage & Invocation (cont.)

- Clear key health check job log example
 - CKDS

```
FOR OF DATA
CHECK(IBMICSF,ICSF_CLEAR_KEYS)
SYSPLEX:    LOCAL    SYSTEM: SY1
START TIME: 02/10/2023 14:15:13.772356
CHECK DATE: 20230111  CHECK SEVERITY: LOW

CSFH0054I Check for clear keys in the CKDS, PKDS, and TKDS

Active CKDS: JLAU.HCR77D2.KDSRL.CKDS
-----
AES.CLEAR.TOKEN.LN16          DATA
AES.CTR.MODE.128K.CLR.KAT     DATA
AES.CTR.MODE.192K.CLR.KAT     DATA
AES.CTR.MODE.256K.CLR.KAT     DATA
AES.CTR.MODE.256K.CLR.KAT     DATA
```


Usage & Invocation (cont.)

- PKDS

```
Active PKDS: JLAU.HCR77E0.KDSRL.PKDS
```

```
-----  
#.HCR77D0.RSAMEVAR.CLEAR.MOD1024
```

```
#JLAU.CLEARKEYHC.QSA
```

```
CCA.CRT08.EXT.CLR.1024S0F
```

```
CCA.CRT08.EXT.CLR.2048S0F
```

```
CCA.PVT06.EXT.CLR.1024S0F
```

- TKDS

```
Active TKDS: JLAU.HCR77D1.KDSR.TKDS
```

```
-----  
$20151204.HCR77C0.KEYAUD.TOKEN 00000000AT
```

```
$20151204.HCR77C0.KEYAUD.TOKEN 00000000BT
```

```
$20151204.HCR77C0.KEYAUD.TOKEN 00000000CT
```

```
$20151204.HCR77C0.KEYAUD.TOKEN 00000000DT
```

```
$20151204.HCR77C0.KEYAUD.TOKEN 00000000ET
```

```
$20151204.HCR77C0.KEYAUD.TOKEN 00000000FT
```

Usage & Invocation (cont.)

* Low Severity Exception *

CSFH0056E Clear keys in the CKDS, PKDS, or TKDS were found.

Explanation: This check detected clear keys in the active key data sets. The label of the records are listed.

System Action: There is no effect on the system.

Operator Response: Contact the ICSF administrator.

System Programmer Response: Contact the ICSF administrator.

Problem Determination: If you are using the common record format (KDSR) of the CKDS, PKDS, or TKDS you may be able to determine if the label is being used in an application.

You should contact your ICSF administrator to determine if any of the clear key(s) should be replaced by secure key(s).

Usage & Invocation (cont.)

Source: n/a

Reference Documentation:

- z/OS Cryptographic Services ICSF Administrators Guide

- z/OS Cryptographic Services ICSF Application Programmers Guide

Automation: n/a

Check Reason: Detects keys that are clear.

Interactions & Dependencies

- Software Dependencies
 - z/OS Health Checker
- Hardware Dependencies
 - None
- Exploiters
 - None

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level:
 - No

Installation & Configuration

- None

Summary

- A health check is added that lists any clear keys found in the active CKDS, PKDS, and TKDS every time ICSF is initialized

Appendix

- Publications
 - IBM Health Checker for z/OS User's Guide
 - ICSF Application Programmer's Guide