SAP Note

3015354 - Setting the SSL Purpose for a Personal Security Environment (PSE) Store Fails With an Error "* 5657: PSE purpose blocked by configuration: Set Purpose SSL is blocked by ini file parameter sslclientpki = on"

Version 3 **Validity:** 25.07.2022 - active **Language** English

Header Data

Released On	25.07.2022 04:34:14 **By** Jinsol Kim (I533393)
Release Status	Released for Customer
Component	HAN-DB-SEC SAP HANA Security & User Management Display ACRF Content
Priority	Correction with high priority
Responsible	Jinsol Kim (I533393)
Processor	Jinsol Kim (I533393)
Category	Consulting
Relevant for Translation	No

Symptom

Setting a purpose for a PSE store fails with an error "* 5657: PSE purpose blocked by configuration: Set Purpose SSL is blocked by ini file parameter sslclientpki = on SQLSTATE: HY000".

Also 'warning' logs similar to the following are written in an indexserver trace:

> [00000]{000000}[00/-1] 0000-00-00 00:00:00.000000 **w** Crypto check_pse_store.cc : Error assigning PSE <PSE_NAME> to purpose 1: exception 1: no.301130 (Crypto/CertAdm/PSEStore/PSEStoreChecker.cpp)
> **Set Purpose SSL is blocked by ini file parameter sslclientpki = on**

Other Terms

PSE (Personal Security Environment), SSL, sslclientpki, Client PKI

Reason and Prerequisites

Issue number 262593

Reason:

As of HANA 2 SPS06, new configuration parameter [communication] sslclientpki is introduced and is set "on" for new installation. And for an upgraded instance, it remains "off" becaues a running instance might already have a custom PSE set up with SSL.

Enabling the Client PKI ([communication] sslclientpki = 'on') at runtime generates two certificates (_SYS_CLIENTPKI_ROOT_CERT and _SYS_CLIENTPKI_HOST_CERT) and two corresponding PSEs (_SYS_CLIENTPKI_ROOT_CA and _SYS_CLIENTPKI). They are generated during system startup as well (only if they don't exist).

By design, system-generated PSE _SYS_CLIENTPKI cannot be used together with a customer PSE with the purpose SSL.

[Example]

1. Enable the Client PKI on **SYSTEM** databaes

> ALTER SYSTEM ALTER CONFIGURATION ('global.ini', 'SYSTEM') SET ('communication', 'sslclientpki') = 'on' WITH RECONFIGURE;

2. Check certificates and PSEs

> SELECT name, purpose, owner_name FROM PSES;

NAME	PURPOSE	OWNER_NAME
_SYS_CLIENTPKI_ROOT_CA	?	SYS
_SYS_CLIENtPKI	**SSL**	SYS
TEST_PSE	?	<DB_USER>

> SELECT pse_name, certificate_name FROM PSE_CERTIFICATES;

PSE_NAME	CERTIFICATE_NAME
_SYS_CLIENTPKI_ROOT_CA	_SYS_CLIENTPKI_**ROOT**_CERT
_SYS_CLIENTPKI	_SYS_CLIENTPKI_**HOST**_CERT
TEST_PSE	TEST_CERTIFICATE

3. Set the purpose SSL for a custom PSE

> SET PSE TEST_PSE PURPOSE SSL;

"PSE purpose blocked by configuration: Set Purpose SSL is blocked by ini file parameter sslclientpki = on SQLSTATE: HY000"

This error is raised because either the system-generated PSE (_SYS_CLIENTPKI) or a custom PSE with the purpose SSL (TSET_PSE) can be used but **not both**. That is, they are ***mutually exclusively***.

Therefore, this is not a product issue, but an expected behavior.

For further detail regarding automatic configuration with the Client PKI, please refer to SAP HANA Security Guide for SAP HANA Platform.

Affected Releases:

- SAP HANA 2:
  - Revisions of SPS06
  - or higher
- or higher

Prerequisites:

1. Configuration parameter [communication] sslclientpki is set to 'on' **AND**
2. A user tries to set the SSL purpose for a user-defined PSE

Solution

In case a user wants to use his or her own PSE with the purpose SSL, the Client PKI first needs to be disabled on ***SYSTEM*** database as follows:

> ALTER SYSTEM ALTER CONFIGURATION ('global.ini', 'SYSTEM') SET ('communication', 'sslclientpki') = 'off' WITH RECONFIGURE;

This will delete certificate _SYS_CLIENTPKI_HOST_CERT and its corresponding PSE _SYS_CLIENTPKI from the system.

> SELECT name, purpose, owner_name FROM PSES;

NAME	PURPOSE	OWNER_NAME
_SYS_CLIENTPKI_ROOT_CA	?	SYS
TEST_PSE	?	<DB_USER>

> SELECT pse_name, certificate_name FROM PSE_CERTIFICATES;

PSE_NAME	CERTIFICATE_NAME
_SYS_CLIENTPKI_ROOT_CA	_SYS_CLIENTPKI_**ROOT**_CERT
TEST_PSE	TEST_CERTIFICATE

Since there remains no PSE with SSL on the system, the purpose SSL now can be set for the custom PSE TEST_PSE.

Note:

If you want to remove PSE _SYS_CLIENTPKI_ROOT_CA and its corresponding certificate _SYS_CLIENTPKI_ROOT_CERT, excute a following SQL command on **SYSTEM** database with the Client PKI disabled:

1. ALTER SYSTEM ALTER CONFIGURATION ('global.ini', 'SYSTEM') SET ('communication', 'sslclientpki') = 'off' WITH RECONFIGURE;

2. ALTER SYSTEM CLIENTPKI DROP ROOT CA;

(Please refer to SAP HANA SQL Reference Guide for SAP HANA Platform for further detail)

Enabling Client PKI at runtime will generate aforementioned certificates and PSEs again.

Validity

Software Component	From Rel.	To Rel.	And Subsequent	
HDB	2.00	2.00		

References

This document refers to:

SAP Knowledge Base Articles

2250144 HAN-DB-SEC FAQ: SAP HANA Secure User Store
2159014 HAN-DB-SEC FAQ: SAP HANA Security

This document is referenced by:

SAP Knowledge Base Articles (1)

2159014 HAN-DB-SEC FAQ: SAP HANA Security