openQA Tests - action #100578

[sle][security][sle15sp4][feature][manual] SLE-21222 - QA: FIPS 140-3: make GnuTLS and Libnettle module ready for certification process

2021-10-07 08:32 - bchou

Status:	New	**Start date:**	2021-10-07
Priority:	Normal	**Due date:**	
Assignee:	bchou	**% Done:**	0%
Category:	New test	**Estimated time:**	0.00 hour
Target version:			
Difficulty:			

Description

https://jira.suse.com/browse/SLE-21222

Prepare GnuTLS and Libnettle modules for certification process under FIPS 140-3 standards. Make all code changes necessary, in GnuTLS and Libnettle, to comply with FIPS 140-3 standards to pass the validation process of NIST and obtain the FIPS certificate for the module.

Confirmed platforms:

```
x86_64 intel
x86_64 AMD
aarch64
s390x zX (exact platform not yet specify)
```

Platforms under evaluation, pending for confirmation:

```
IBM Power 9/10
```

Algorithms:

7 algorithms

```
AES
DRBG
DSA
ECDSA
HMAC
RSA
SHS
```

*Note that we identified 8 algorithms at the beginning, including Triple-DES, however we decided to not include it due to its sunset in 2022.

Standards:

The standards to follow are the FIPS 140-3. See:

https://confluence.suse.com/download/attachments/411795603/140-3_SUSE_RA.pdf?version=1&modificationDate=1618334281277&api=v2

https://www.atsec.com/wp-content/uploads/2020/11/atsec_FIPS-140-3_vs_140-2.pdf

https://csrc.nist.gov/projects/fips-140-3-transition-effort