

# Network Device Interpretation # 202011

## Clarification about FIA\_AFL.1

**Status:**  *Active*  *Inactive*

**Date:** 14-Sep-2020

**End of proposed Transition Period (to be updated after TR2TD process):** 14-Sep-2020

**Type of Change:**  Immediate application  Minor change  Major change

**Type of Document:**  *Technical Decision*  *Technical Recommendation*

**Approved by:**  *Network iTC Interpretations Team*  *Network iTC*

**Affected Document(s):** ND cPP v2.1; ND cPP v2.2e

**Affected Section(s):** FIA\_AFL.1

**Superseded Interpretation(s):** None

### Issue:

The customer supports public-key based authentication. Password based authentication is not being claimed for SSH as part of FCS\_SSHC\_EXT.1.2/FCS\_SSHS\_EXT.1.2.

The requirements of the SFRs are as follows:

FCS\_SSHC\_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [selection: password-based, no other method].

FCS\_SSHS\_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [selection: password-based, no other method].

The TD0409: NIT decision for Applicability of FIA\_AFL.1 to key-based SSH authentication states that FIA\_AFL.1 is only mandatory for password-based authentication.

Application notes: If the TOE supports password-based authentication, the option 'password-based' shall be selected. If the TOE supports only public key-based authentication, the option 'no other method' shall be chosen.

### Question:

In the above scenario, where only public key based authentication is supported, is there a requirement to include FIA\_AFL.1 in the scope of the evaluation?

Please clarify on what updates are required in the ST to address the non-applicability of FIA\_AFL.1 when only public-key based authentication is supported. At present it is unclear on what the corrective action should be for the ST. Can the SFR be omitted from the ST where only public key authentication is supported in FCS\_SSHS\_EXT.1.2/FCS\_SSHC\_EXT.1.2?

**Resolution:**

1. FIA\_AFL.1 is a mandatory SFRs that the TOE will need to meet.
2. FIA\_AFL.1 requires at least one remote administrative interface support password authentication.
3. If SSH is the TOE's only remote administrative interface, it needs to support password authentication. If there is another administrative interface (e.g. a web GUI) that supports password authentication, SSH does not need to support password authentication and, by extension, FIA\_AFL.1

**Rationale:**

Exact conformance mandates that all mandatory SFRs are implemented by a TOE.

**Further Action:**

In future versions of the cPP, models of authentication need to be reviewed and revamped to consider different use cases and enterprise deployment scenarios.

**Action by Network iTC:**

*None*