Network Device Interpretation # 201702a rev2

Making DH Group 14 optional in FCS_IPSEC_EXT.1.11

Status: ☒ *Active* ☐ *Inactive*

Date: *10-May-2017*

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

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

Affected Document(s): *NDcPP V1.0, FWcPP V1.0*

Affected Section(s): *FCS_IPSEC_EXT.1.11, FCS_CKM.2.1*

Superseded Interpretation(s): *201702a, 31-Mar-2017*

Issue:

References

[FWcPPv1.0]	https://www.niap-ccevs.org/pp/cpp_fw_v1.0.pdf
[NDcPP]	https://www.niap-ccevs.org/pp/cpp_nd_v1.0.pdf
[RFC3526]	https://www.ietf.org/rfc/rfc3526.txt
[RFC4253]	https://www.ietf.org/rfc/rfc4253.txt
[FIPS 186-4]	http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

Issues

The vendor must design their products to meet [RFC4253] and [RFC3526] as required by [FWcPP and NDcPP].

[FWcPP and NDcPP]

> *FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, **4253**, 4254, and [selection: 5647, 5656, 6187, 6668, no other RFCs].*

[RFC4253, section 8.2]

> 8.2. diffie-hellman-group14-sha1
>
> The "diffie-hellman-group14-sha1" method specifies a Diffie-Hellman key exchange with SHA-1 as HASH and Oakley Group 14 [**RFC3526**] (2048-bit MODP Group), and it MUST also be supported.

[RFC3526, page 3]

```
3.  2048-bit MODP Group

   This group is assigned id 14.

   This prime is: 2^2048 - 2^1984 - 1 + 2^64 * { [2^1918 pi] + 124476 }

   Its hexadecimal value is:

      FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1
      29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD
      EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245
      E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED
      EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D
      C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F
      83655D23 DCA3AD96 1C62F356 208552BB 9ED52907 7096966D
      670C354E 4ABC9804 F1746C08 CA18217C 32905E46 2E36CE3B
      E39E772C 180E8603 9B2783A2 EC07A28F B5C55DF0 6F4C52C9
      DE2BCBF6 95581718 3995497C EA956AE5 15D22618 98FA0510
      15728E5A 8AACAA68 FFFFFFFF FFFFFFFF

   The generator is: 2.
```

In [RFC3526] or "MODP Diffie-Hellman groups for IKE", the RFC specifies precomputed domain parameters (p and g) to be used for the DH group 14 exchange. These values do not need to be a secret but must be the same value for both peers. However, FCS_CKM.2[1] forces the vendor to generate the FFC domain parameters according to [FIPS 186-4] "Digital Signature Standard (DSS)". This could cause an interoperability issue if the peer does not support the same FFC domain parameters expected to establish the trusted path. Forcing Diffie-Hellman group 14 in FCS_IPSEC_EXT.1.11 while the product already supports stronger ECC groups should not be necessary. In addition, draft NDcPPv2.0 already makes DH-Group 14 a selection option.

FCS_IPSEC_EXT.1.11 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: *19 (256-bit Random ECP), 5 (1536-bit MODP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), no other DH groups*].

Proposal

Due to the inconsistency and interoperability issue, we propose making DH group 14 exchange **NOT** mandated in the [FWcPP and NDcPP] for IPSec.

FCS_IPSEC_EXT.1.11 The TSF shall ensure that all IKE protocols implement DH Group(s) [selection: *14 (2048-bit MODP), 19 (256-bit Random ECP), 5 (1536-bit MODP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP)*].

[1] In application note, "The domain parameters used for the finite field-based key establishment scheme are specified by the key generation according to FCS_CKM.1.1."

In the updated SFR, DH group 14 exchange is not removed but was made selectable. Removing it may affect other international standard. This is also consistent with FCS_SSHS_EXT.1.7 and FCS_SSHC_EXT.1.7 where DH group 14 exchange is selectable.

Resolution:

The NIT acknowledges the problem specified in the Issue section. FCS_IPSEC_EXT.1.11 shall therefore be modified as follows:

"**FCS_IPSEC_EXT.1.11** The TSF shall ensure that IKE protocols implement DH Group(s) [selection: *14 (2048-bit MODP), 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP)*]."

The application note related to FCS_IPSEC_EXT.1.11 shall be modified as follows:

"The selection is used to specify DH groups supported. This applies to IKEv1 and IKEv2 exchanges."

The corresponding sections in the extended component definition have to be updated accordingly.

This TR deals with one part of the issue raised by RfI#201702, however from the NIT's perspective this change does not fully resolve the issue because the conflict with the requirements defined in FCS_CKM.2 remains if an ST author selects DH group 14. Therefore the NIT will propose a change to FCS_CKM.2 to resolve this issue in a separate Technical Recommendation RfI#201702b.

Rationale:

As stated in the 'Issue' section. Note that DH group 5 has been removed as a selectable option from FCS_IPSEC_EXT.1.11 due to its insufficient security strength as well as its incompatibility to NIST SP800-56Arev2.

Further Action:

None

Action by Network iTC:

None