

strongSwan - Feature #2367

Android client - RSASSA-PSS

24.06.2017 22:53 - Hans Muster

| | |
|---|----------------------------------|
| Status: Closed | Start date: 24.06.2017 |
| Priority: Normal | Due date: |
| Assignee: Tobias Brunner | Estimated time: 0.00 hour |
| Category: android | |
| Target version: 5.7.0 | |
| Resolution: Fixed | |
| Description | |
| RFC 7427 and BSI TR-02102-3 (german only): https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index.htm.html recommend the newer RSASSA-PSS method for authentication with RSA digital signatures. RFC 7427, chapitre 1: <i>In IKEv2, authentication using RSA digital signatures calls for padding based on RSASSA-PKCS1-v1_5, although the newer RSASSA-PSS padding method is now recommended.</i> It looks like StrongSwan Android App v1.8.2 don't support secure RSASSA-PSS with SHA-256 (see RFC 7427, chapitre A4.3). StrongSwan Android App v1.8.2 supports only the less secure RSASSA-PKCS1-v1.5 with SHA-256 (sha256WithRSAEncryption => see RFC 7427, chapitre A.1.2). Could you please add (for security reasons) RSASSA-PSS support to StrongSwan Android App. Thank you. | |
| Related issues: | |
| Related to Feature #2427: Implementing RFC 8247 | Closed |

History

#1 - 26.06.2017 10:06 - Tobias Brunner

- Status changed from New to Feedback

strongSwan currently does not support RSASSA-PSS. Until it does the Android client won't support it either.

#2 - 19.09.2017 12:03 - Tobias Brunner

- Related to Feature #2427: Implementing RFC 8247 added

#3 - 01.01.2018 15:11 - Hans Muster

StrongSwan Android App v1.9.5 works with StrongSwan v5.6.1. StrongSwan v5.6.1 should support RSASSA-PSS signatures:

<https://wiki.strongswan.org/versions/67>

Feature [#2427](#)

But StrongSwan Android App v1.9.5 doesn't support RSASSA-PSS signatures. Is there a secret/hidden way to activate RSASSA-PSS support in StrongSwan Android App v1.9.5. Thank you.

#4 - 21.06.2018 15:48 - Tobias Brunner

- *Category set to android*
- *Status changed from Feedback to Closed*
- *Assignee set to Tobias Brunner*
- *Target version set to 5.7.0*
- *Resolution set to Fixed*