strongSwan - Feature #2427

Implementing RFC 8247

13.09.2017 21:46 - Noel Kuntze

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:			
Target version:	5.6.1		
Resolution:	Fixed		

Description

RFC 8247 mandates that support for certain algorithms is removed and for certain others is added for IKEv2:
Removed: E.g. prf-md5, hmac-md5, null encryption, modp1024s160, modp768
Added: E.g. RSASSA-PSS

Somebody will ineviteably ask for it.

Related issues:

Related to Feature #2367: Android client - RSASSA-PSS	**Closed**	**24.06.2017**

Associated revisions

Revision 10da451f - 08.11.2017 16:47 - Tobias Brunner

proposal: Remove MD5 from default IKE proposal

RFC 8247 demoted MD5 to MUST NOT.

References #2427.

Revision 76c58498 - 08.11.2017 16:47 - Tobias Brunner

proposal: Remove MODP-1024 from default IKE proposal

RFC 8247 demoted it to SHOULD NOT. This might break connections with
Windows clients unless they are configured to use a stronger group or
matching weak proposals are configured explicitly on the server.

References #2427.

Revision 43b59d13 - 08.11.2017 16:47 - Tobias Brunner

ikev2: Don't use SHA-1 for RFC 7427 signature authentication

RFC 8247 demoted it to MUST NOT.

References #2427.

Revision 1c4b392a - 08.11.2017 16:53 - Tobias Brunner

Merge branch 'rsassa-pss'

This adds support for RSASSA-PSS signatures in IKEv2 digital signature
authentication (RFC 7427), certificates and CRLs etc., and when signing
credentials via pki tool. For interoperability with older versions, the
default is to use classic PKCS#1 signatures. To use PSS padding either enable
rsa_pss via strongswan.conf or explicitly use it either via ike:rsa/pss...
auth token or the --rsa-padding option of the pki tool.

References #2427.

History

#1 - 19.09.2017 12:03 - Tobias Brunner

- Related to Feature #2367: Android client - RSASSA-PSS added

#2 - 08.11.2017 17:05 - Tobias Brunner

- Tracker changed from Issue to Feature

- Status changed from New to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.6.1

- Resolution set to Fixed