IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Security Inputs to IEEE 802.11 TGai | | | | |
| Date: January 19, 2012 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| René Struik | Struik Security Consultancy | 723 Carlaw Avenue  Toronto ON  Canada M4K 3K8 | USA: +1 (415) 690-7363  Toronto: +1 (647) 867-5658  Skype: rstruik | rstruik.ext@gmail.com |

Device joining shall include an authentication scheme, where two devices A and B derive a shared key (key agreement) and show that these have computed correctly (key confirmation) in each of the following scenarios:

1. Both devices do not share a secret key, but each shares a key with a mutually trusted third party.
2. Both devices do have (access to) a certificate of their public key, issued by a trusted third (certificate authority).
3. Both devices do share a weak secret key.
4. Both devices do share a secret key.

Authenticated key agreement schemes shall include the following properties:

1. Key establishment
2. Key Agreement
3. Implicit key authentication
4. Explicit key authentication
5. No unilateral key control
6. Forward secrecy
7. Entity authentication
8. Unknown Key Share Resilience

Security properties should include:

1. Identity protection

Further considerations:

1. Schemes shall be demonstrably free of known security weaknesses (burden on proposers)
2. Schemes shall be well-studied by the cryptographic community
3. Schemes should be standardized via internationally accepted cryptographic standards (NIST/FIPS series, IETF)

Authorization of the STA may include involvement of a third party, where

1. The third party providing authorization may be different from a third party potentially providing authentication support.