IEEE P802.11
Wireless LANs

|  |
| --- |
| Specification Framework for TGai |
| Date: 2012-03-15 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Tom Siep | CSR | 3779 Pecan Acres Drive, Farmersville, TX, USA | +1 214 558 4358 | Tom.Siep@CSR.com |
| Marc Emmelmann | Fraunhofer FOKUS | Kaiserin-Augusta-Allee 3110589 Berlin GERMANY | +49 30 34637268 | emmelmann@ieee.org |
| Hiroshi MANO | AlliedTelesisRD Center K.K.Root Lab | 8F TOC2 Bldg. 7-21-11 Nishi-Gotanda, Shinagawa-ku, Tokyo 141-0031 JAPAN | +81-3-5436-8350 | hmano@root-hq.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This document provides the framework from which the draft TGai amendment will be developed. The document provides an outline of each of the functional blocks that will be a part of the final amendment. The document is intended to reflect the working consensus of the group on the broad outline for the draft specification. As such it is expected to begin with minimal detail reflecting agreement on specific techniques and highlighting areas on which agreement is still required. It may also begin with an incomplete feature list with additional features added as they are justified. The document will evolve over time until it includes sufficient detail on all the functional blocks and their inter-dependencies so that work can begin on the draft amendment itself.

As this document evolves, the most recent changes will be in track-change format. Older changes will be converted to normal text.

**Revision notes**

***R2:*** *Initial version accepted by 802.11ai TG*

*R4: Changes on 12 March 2012*

*R5: Changes on 13 March 2012*

*R6: Changes including 14 Mar. 2012*

*R7: Ides of March 2012 changes, plus corrections discovered upon review*

*R8: May 2012 update*

*R9 Changes from 16 & 17 July*

*R10 Editorial smoothing; updated references*

# Definitions

**Link Setup**: the process of gaining the ability to send IP traffic with a valid IP address through the AP. Link Setup may involve more than one AP in an ESS. This includes AP/Network discovery and (secure) Association and Authentication. [1]

**Link-Attempt Rate** is the number of STAs attempting to establish a link for the first time to an AP within an ESS as measured over a one second time interval.

**Media Load** is the “busyness” of the wireless medium of the ESS. It is measured as the percentage of time the medium is in use.

**Link Setup Time** is defined as the process of gaining the ability to send IP traffic with a valid IP address through the AP. Link Setup may involve more than one AP in an ESS. This includes AP/Network discovery and (secure) Association and Authentication. Link Setup Time is the amount time required in the use case to establish link setup. Timing starts when the STA elects to perform Link Setup.

# Abbreviations and acronyms

**FILS** Fast Initial Link Setup

HLCF Higher Layer Configuration Function (The nature of HLCF is TBD)

# Link Setup General Framework

## Optimizations (11-12/0160-03)

A TGai solution may allow AP and STA to initiate link setup optimizations.

(11-12/0655r5) The TGai amendment shall accommodate efficient use of other FILS features when L3 setup cannot be completed concurrently with authentication.

## HLCF Indications (11-12/0359r6)

The HLCF capability of the AP shall be indicated in Beacon and Probe Response.

## Encapsulation Framework for HLCF (11-12/0655r5)

The TGai amendment defines a generalized method for upper layer transport encapsulation during FILS to enable higher layer services.Security Framework

## Pre-established security context (11-12/159r5)

11ai should support faster authentication using pre-established security data setup between the STA and the network

The draft specification shall include (11-12/0907r05)

* Support for the EAP-RP [as defined in IETF RFC 5295/5296] for fast key establishment.
* A nonce exchange and key confirmation that does not degrade the security of the 4-way handshake.

The draft specification shall include optional support of Perfect Forward Secrecy as part of key establishment. (11-12/0907r05)

The draft specification shall include support for a FILS authentication mechanism that does not require online involvement of a third party for authentication (of course, it may involve it for authorization and does not preclude online involvement for authentication). (11-12/0907r05)

The draft specification shall include support for a public-key based authenticated key agreement scheme as a mechanism for fast FILS authentication. (11-12/0907r05)

The draft specification shall include support for a public-key based authenticated key agreement scheme based on NIST approved schemes using ECDH and ECDSA at 128-bit cryptographic bit strength. (11-12/0907r05)

## Concurrent operations (11-12/159r5)

11ai should support optimized message exchanging for association, authentication and key establishment.

## Authentication (11-12/0157r8)

The draft should include an authentication scheme, where STA and AP derive a shared key (key agreement) and show that these have computed correctly (key confirmation), where both devices do not share a secret key, but each shares a distinct key with a mutually trusted third party AS.

## Security Properties (11-12/0157r8)

The authentication scheme(s) in the draft shall provide the following security properties:

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

Here, properties are provided mutually.

## Cryptographic Strength (11-12/0157r8)

The authentication scheme(s) in the draft SHALL have cryptographic strength of at least 80 bits and SHOULD have cryptographic strength of 128 bits.

## Additional Information (11-12/0157r8)

The authentication scheme(s) should provide for the optional inclusion of additional information in their protocol flows, so as to assist in conveying this information in parallel and logically tied to the protocol.

## State machine update (need reference)

The draft specification shall include support for a revised 802.11 state machine to enable the FILS authentication and association.

## Active and Passive Attack

The mutual authentication protocol in the draft shall be resistant to active and passive attack. If the pre-existing credential is a shared secret, then either:

1. the protocol shall be defined to require that the probability of guessing the secret shall be no more than 2-80 ; or,
2. the protocol shall be resistant to dictionary attack.

## Key Confirmation

The draft specification shall not specify confirmation of a key prior to both parties possessing the key to confirm. (11-12/0907r05)

# IP Address Assignment

## IP version support (11-12/359r6)

The HLCF shall support IPv4 and IPv6.

## Indication of availability of IP Address assignment (11-12/0655r5)

The TGai amendment defines a method to enable a non-AP STA to know availability of IP Address assignment in advance of the TGai association process.

## Compatibility with Dynamic Authorization (11-12/0655r5)

FILS IP address assignment shall accommodate cases where IP address assignment cannot be completed concurrent with authentication.

# Fast Network Discovery

## Active scanning

### Immediate Reporting (11-12/0153r9)

802.11ai shall define a mechanism to optimise the MLME-SCAN.confirm primitive to indicate the discovered APs fast and without additional delays.

### FILS Capability Indication (11-12/0153r9)

Probe Request, Probe Response and Beacon shall contain an indication of FILS capability.

### Probe Response (11-12/0153r9)

802.11ai shall have mechanism to transmit Probe Response frame to individual and/or broadcast address.

### BSS Information on Other Channels (11-12/0153r9)

802.11ai shall have mechanism to include information of the responding AP and other APs to the Probe Response frame.

### Probe Response Collision Avoidance (11-12/0153r9)

An AP may respond to multiple Probe Requests from one or more FILS capable STAs with a single broadcast addressed response frame.

### Ommision of Probe Response (11-12/0153r9)

An FILS Capable AP may omit transmission of Probe Response frame to FILS capable STAs if the TBTT occurs within a predefined time interval.

(11-12/0655r5) Probe request may contain new information that would enable an AP to make the decision whether to respond to a probe request. Examples of this kind of information include:

* Link Quality parameters
* AP Capabilities
* QoS Requirement
* Address/ID

### Listening Duration (11-12/0158r3)

STA may include a wait-time-for-Probe-Response element to Probe Request to provide a max listening duration for which the STA indicates it will wait for Probe Response transmission.

### White List Element in GAS (11-12/0158r3)

STA may include an inclusion selection filter or ‘white’ list element to GAS Request to indicate selection for a set of APs to be included as part of Neighbor Report ANQP element in GAS Response

### Omission of Probe Request (11-12/0655r5)

STA may omit a probe request due to reception of , for example,

* Broadcast probe requests
* Broadcast probe responses
* Beacon

## Passive Scanning

### General Approach (11-12/0406r1)

The 802.11ai shall support improved passive scanning mechanisms to facilitate fast initial link setup, and/or to reduce the air time occupancy of MAC frames used for scanning.

(11-12/0655r5) The AP may transmit a MAC frame, to be defined as “FILS Discovery Frame”, between full Beacon instances to support a quick AP/Network Discovery for a fast initial link setup.

The FILS Discovery Frame may be transmitted periodically and/or non-periodically.

If transmitted periodically, the periodicity of the FILS Discovery Frame may be changed.

The interval between regular beacon and FILS Discovery Frame shall be no less than dot11aiFILSBeaconMinimumInterval.

The FILS Discovery Frame is a public action frame, which is one of the following:

* a Modified Measurement Pilot frame, or
* a Modified 11ah short beacon frame, or
* a newly designed MAC public action frame.

### Power Consumption (11-12/0406r1)

Reducing power consumption of the passive scanning non-AP STAs is desirable.

### Configuration Change Element (11-12/0158r3)

AP may include a GAS configuration-change element in the Beacon and Probe Response to indicate changes in a set of static GAS parameters.

### AP Availability Indicator (11-12/0158r3)

AP may include an indicator for AP availability to attachment to the Beacon and Probe Response.

**References:**

[0] IEEE Std 802.11-2012

[1] 11-10/0238: TGai Use Cases

[2] 11-11/0811: TGai Evaluation Methodology

[3] 11-11/0745: TGai Functionl Requirements