Security Requirements for TGai

- **Date: 2011-11-1**

Authors:

Name	Affiliations	Address	Phone	email
Robert Sun	Huawei Technologies Co., Ltd.	Suite 400, 303 Terry Fox Drive, Kanata, Ontario K2K 3J1	+1 613 2871948	Rob.sun@huawei.com
Yunbo Li	Huawei Technologies Co., Ltd.	F1, Huawei Industrial Base, Bantian Longgang, Shenzhen 518129, China	+86 15013596057	liyunbo@huawei.com
Edward Au	Huawei Technologies Co., Ltd.	Suite 400, 303 Terry Fox Drive, Kanata, Ontario K2K 3J1	+1 773 782 6875	Edward.au@huawei.com
Phil Barber	Huawei Technologies Co., Ltd.	1700 Alma Rd, Ste 500 Plano, Texas 75075 USA	+1 972-365-6314	pbarber@huawei.com

Abstract

This proposal provides the security requirements of the TGai which entail a number of desired properties to satisfy the performance target of TGai.

Conformance w/ Tgai PAR & 5C

Conformance Question	Response
Does the proposal degrade the security offered by Robust Security Network Association (RSNA) already defined in 802.11?	No
Does the proposal change the MAC SAP interface?	No
Does the proposal require or introduce a change to the 802.1 architecture?	No
Does the proposal introduce a change in the channel access mechanism?	No
Does the proposal introduce a change in the PHY?	No
Which of the following link set-up phases is addressed by the proposal? (1) AP Discovery (2) Network Discovery (3) Link (re-)establishment / exchange of security related messages (4) Higher layer aspects, e.g. IP address assignment	3

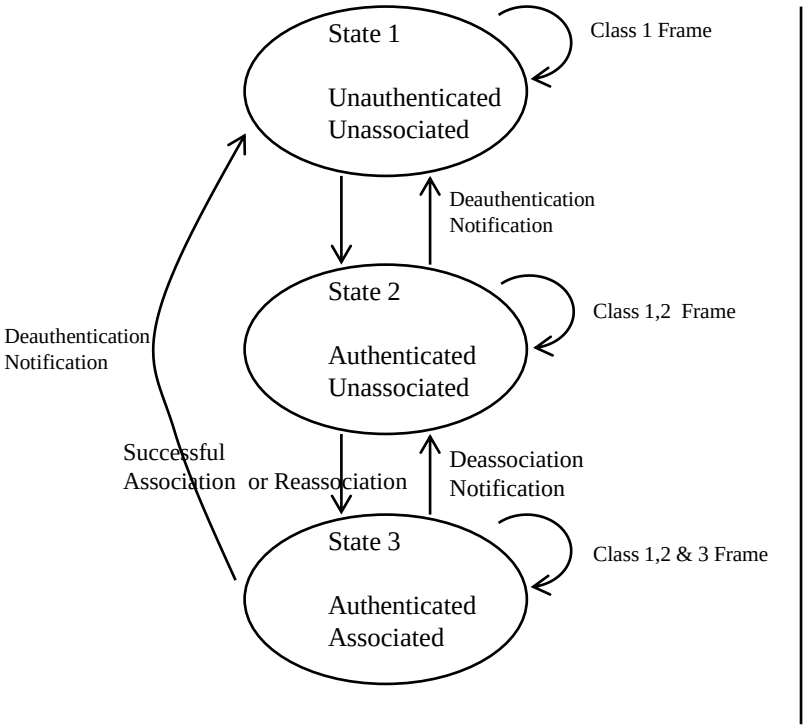
Desired Security Properties for TGai

- **The security system of TGai shall demonstrate efficiency in terms of:**
  - Less round of message exchange in key agreement
  - Less power consumption
  - Less computation complexity
  - Possibility of pre-computation
- **The security system of TGai shall follow the security properties of RSNA**
- **The security system of TGai shall achieve the Perfect Forward Secrecy (PFS) at full authentication state**
  - Compromise a single derived session key suite can only permit access to the data protected by this session key, no compromise in the previous data communication session.
- **The security system of TGai shall achieve the Known-key security which means if some session keys are compromised, future sessions should still be protected with future session keys**

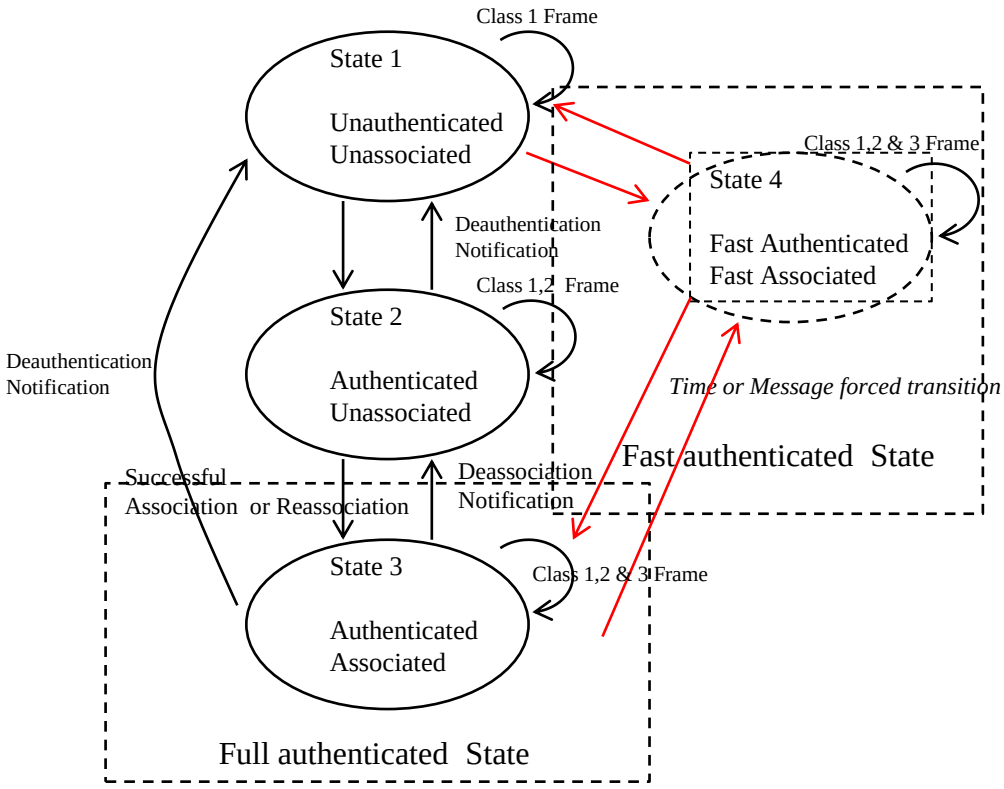
Desired Security Properties for TGai

- **The security system of TGai shall allow reduced PFS or weak PFS at the fast-association state**
  - In order to achieve the target of fast initial link setup with less round of key agreement, the security system at the fast-authentication state may tolerate some sacrificed Perfect Forward Secrecy (PFS) which allows some key materials to be re-used in some message exchange (TBD)
- **The security system of TGai shall provide the assurance of Impersonation key compromise, including the following potential attacks:**
  - MAC address spoofing (Countermeasures are required)
  - Key deleting/injecting (MAC is required)
  - Unkown Key Sharing (Mutual authentication is required)
- **The security system of TGai shall provide sufficient capacity to handle simultaneous fast association/authentication request/response**

Modified Security State Machine



Today's 802.11 security state machine



802.11ai security state machine

State 4 Properties (Mc'Donald State)

- **Device at State 4, it allows Class 1,2 and 3 frames to be transmitted**
- **Device at State 4, it will be upon elapsed timer or special messages to be forced into state 3 or state 1**
- **At State 4, it will maintain that FAST Security Association (FSA) with key materials for both Device and AP**

Questions & Comments