1/23/07

802.11 i

RSN - Robust Security Network

802.11 Wi-Fi Alliance

Wi-Fi Alliance

- Test Plan
TSN - Transitional Security Network

WEP, RSN

Software implementation based on Wi-Fi product

TKIP - Temporal Key Integrity Protocol

RSN, Wi-Fi Alliance

TKIP → WPA Protected Access
RSN - Flexibility
AES
TKIP

WPA - TKIP

RSN & WPA - Support
Same architecture

Architecture

(1) Upper-Level Authentication
(2) Secret Key Distribution
(3) Key renewal

Master Key
Authentication Process - Security Context
Message Protection (integrity & privacy)
Temporal Key
Security Architecture

Three Layers

Wireless LAN Layer
Access Control Layer
Authentication Layer

Access point
IEEE 802.1X
For Access Control
Port Access Control

TLS - Transport Layer Security

Authentication Server

Computational Network

Authentication

Wireless LAN

Access Point

Access Control

O.S.

Supplicant

Wireless LAN

Mobile Device
Access Point

Authentication server

Wired Network

Wireless Network protocol

Mobile

Upper layers will be the same

Lower layers will be different

↓

802.3

or other protocol

↓

TCP/IP

802.1x

EAPOL

EAP - Extensible Authentication Protocol.