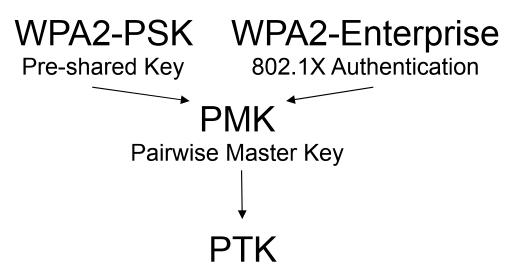


## WPA2 Key Hierarchy



Pairwise Transient Key generated during **4-way handshake** unique for each association between AP and STA

|PTK|=384 bits (3\*128 bits): KCK || KEK || TK

## GMK Group Master Key randomly generated by AP

**Group Transient Key** 

- Temporary key for broadcast and multicast by AP
- Updated every time the group changes (a STA leaves or joins)

Key Confirmation Key
authentication key
used for MIC computations in
4-way-handshake
(MIC = message integrity code)

Key Encryption Key encryption of 4-way-hanshake and of new (and updated) GTK



## Four-Way Handshake

