EAP-PSK: a simple symmetric key EAP method

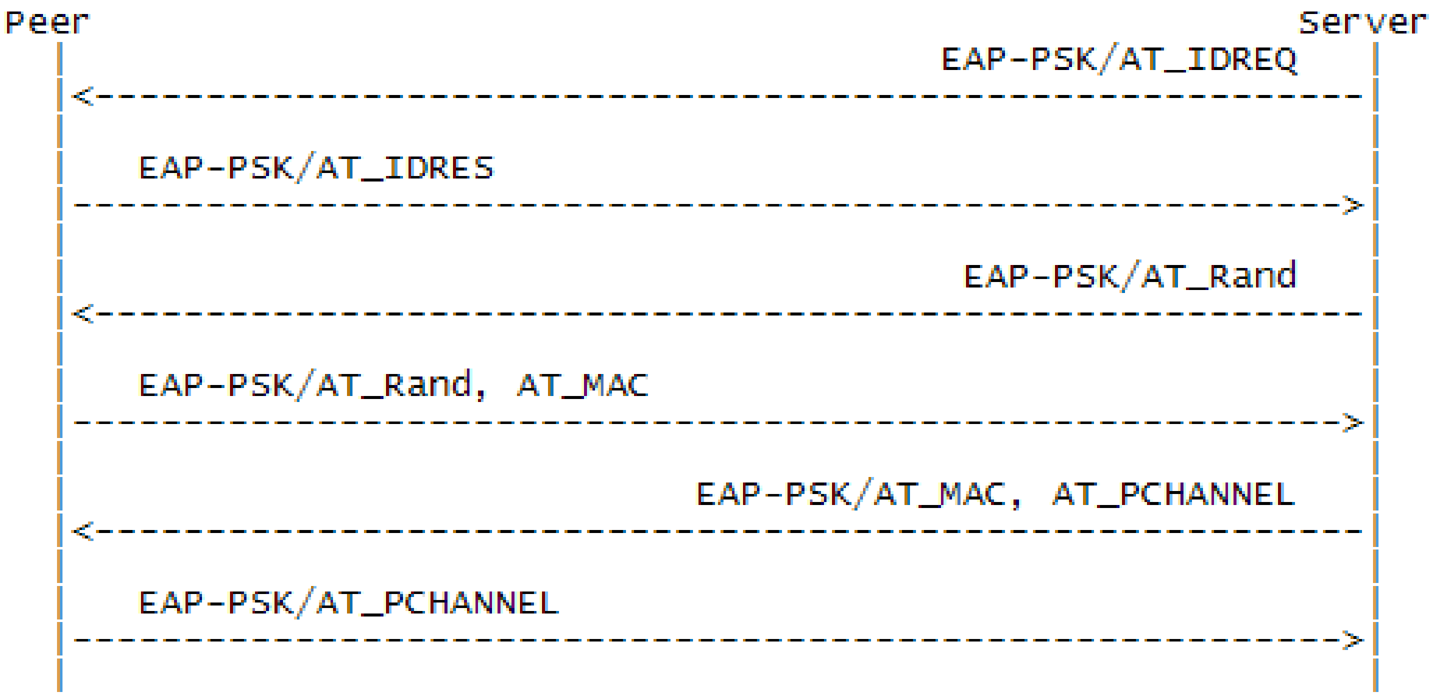
IETF 59 – Seoul, Korea

March 2004

EAP-PSK: providing a simple & secure symmetric key EAP method

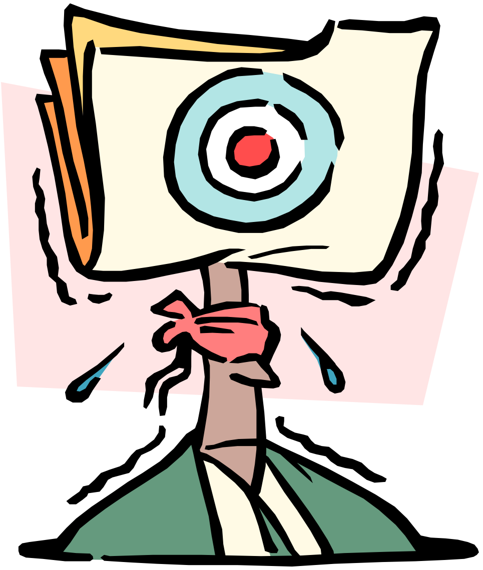
- EAP-PSK relies on symmetric cryptography and uses AES-128 as its sole primitive
- EAP-PSK is designed (as most contemporary EAP methods) with WLANs in mind
- EAP-PSK is currently being implemented and implementation source will be released
- EAP-PSK should be mature by next IETF (July 2004)
- Intent is to request publication as Informational although Standards track could be an option
- EAP-PSK is a proposition made to gather momentum for the (quick) design of a single pre-shared key EAP method

EAP-PSK overview



```
Peer                                                        Server
 |                                          EAP-PSK/AT_IDREQ   |
 |<----------------------------------------------------------- |
 |                                                             |
 |  EAP-PSK/AT_IDRES                                           |
 |-----------------------------------------------------------> |
 |                                                             |
 |                                           EAP-PSK/AT_Rand   |
 |<----------------------------------------------------------- |
 |                                                             |
 |  EAP-PSK/AT_Rand, AT_MAC                                    |
 |-----------------------------------------------------------> |
 |                                                             |
 |                              EAP-PSK/AT_MAC, AT_PCHANNEL    |
 |<----------------------------------------------------------- |
 |                                                             |
 |  EAP-PSK/AT_PCHANNEL                                        |
 |-----------------------------------------------------------> |
 |                                                             |
```

Any feedback welcome!



Florent Bersani, France Telecom R&D

florent.bersani@francetelecom.com

Backup slides

EAP-PSK design goals

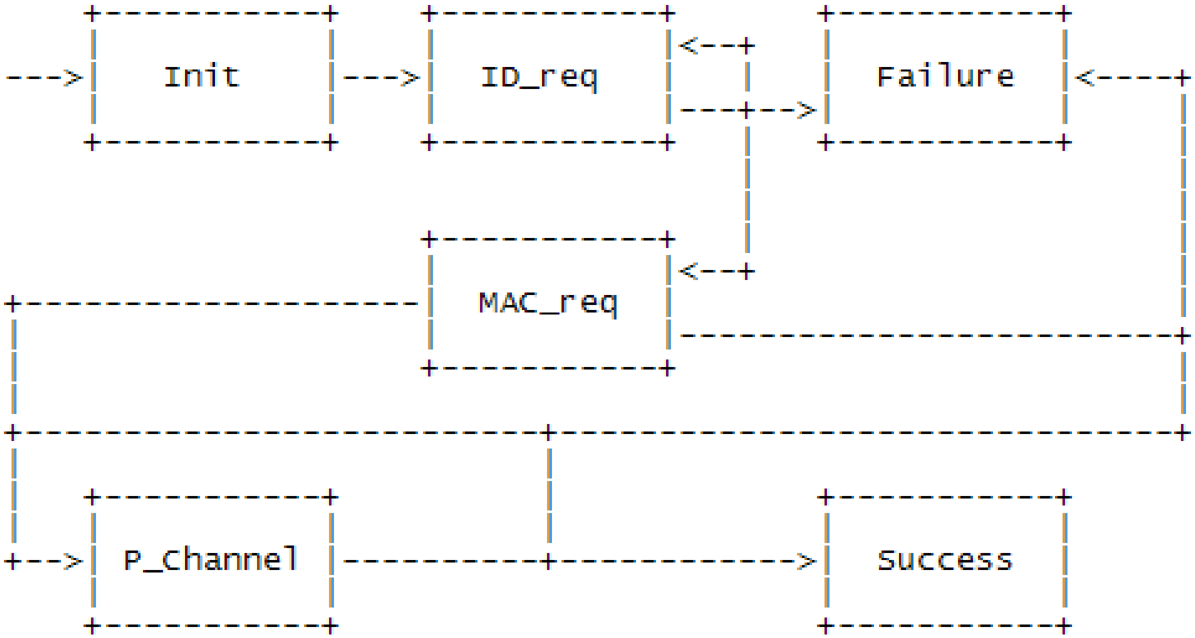
- **Simplicity**: It should be easy to implement and to deploy without any pre-existing infrastructure.
- **Wide applicability**: It should be possible to use this method to authenticate over any network. In particular, it should be suitable for [IEEE 802.11] wireless LANs and comply to [IEEE 802REQ]
- **Security**: It should be conservative in its cryptographic design and enjoy security proofs
- **Extensibility**: It should be possible to add to this method the required extensions as their need appears
- **Patent-avoidance**: It should be free of any Intellectual Property Right claims

EAP-PSK related work

- EAP-Archie: very close but EAP-Archie will not be further developed*
- EAP-SKE: ongoing effort to merge (possible problem: patent encumbrance of EAP-SKE)
- LEAP: security flaws
- EAP-FAST: less lightweight (tunneling,…)
- …

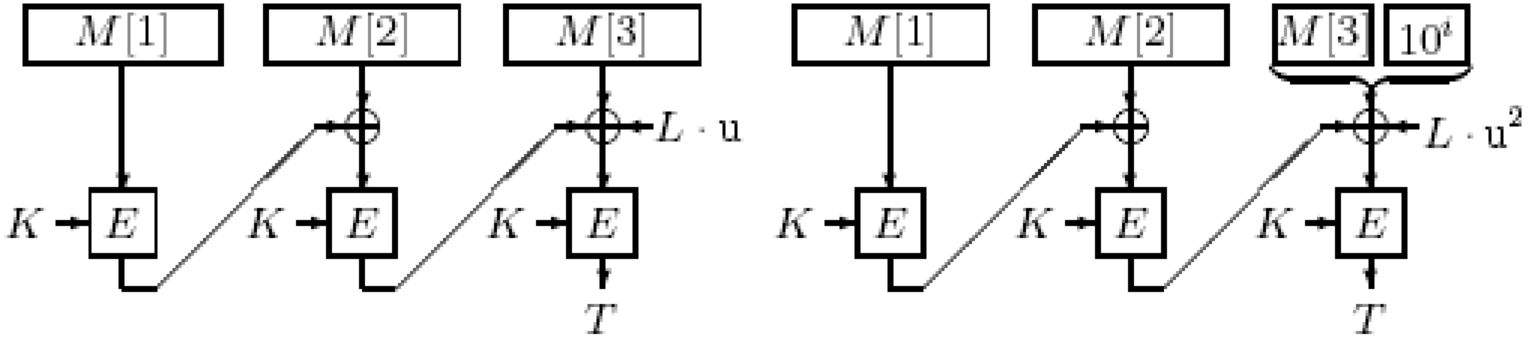
Source: Jesse Walker & Russ Housley, personal communication, 2004

EAP-PSK peer state machine



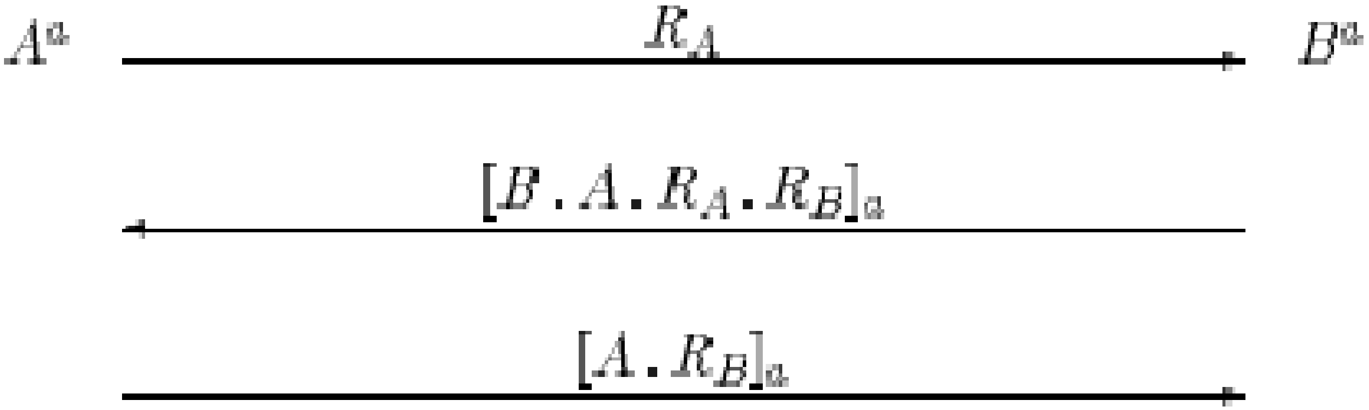
```
    +-----------+    +-----------+       +-----------+
    |           |    |           |<--+   |           |
--->|   Init    |--->|  ID_req   |   |   |  Failure  |<----+
    |           |    |           |---+-->|           |     |
    +-----------+    +-----------+   |   +-----------+     |
                                     |                     |
                                     |                     |
                     +-----------+   |                     |
                     |           |<--+                     |
+--------------------|  MAC_req  |                         |
|                    |           |-------------------------+
|                    +-----------+                         |
|                                                          |
+--------------------------+-------------------------------+
|                          |
|   +-----------+          |             +-----------+
|   |           |          |             |           |
+-->| P_Channel |----------+------------>|  Success  |
    |           |                        |           |
    +-----------+                        +-----------+
```

OMAC1



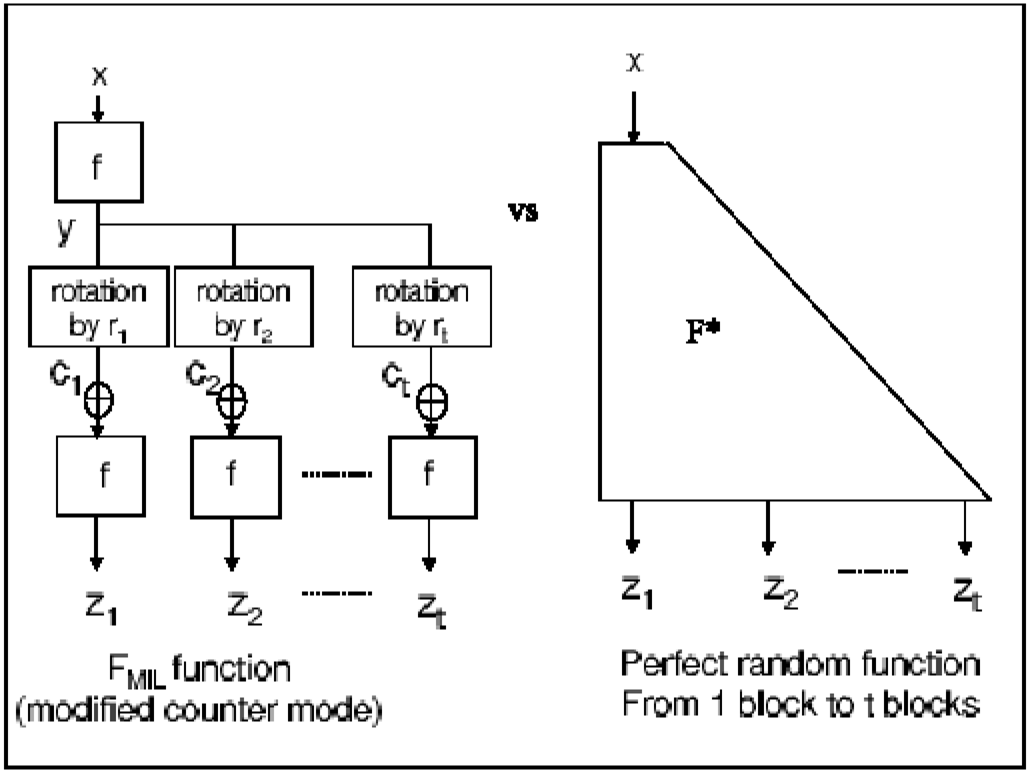
Source: [OMAC], Figure 2

MAP1



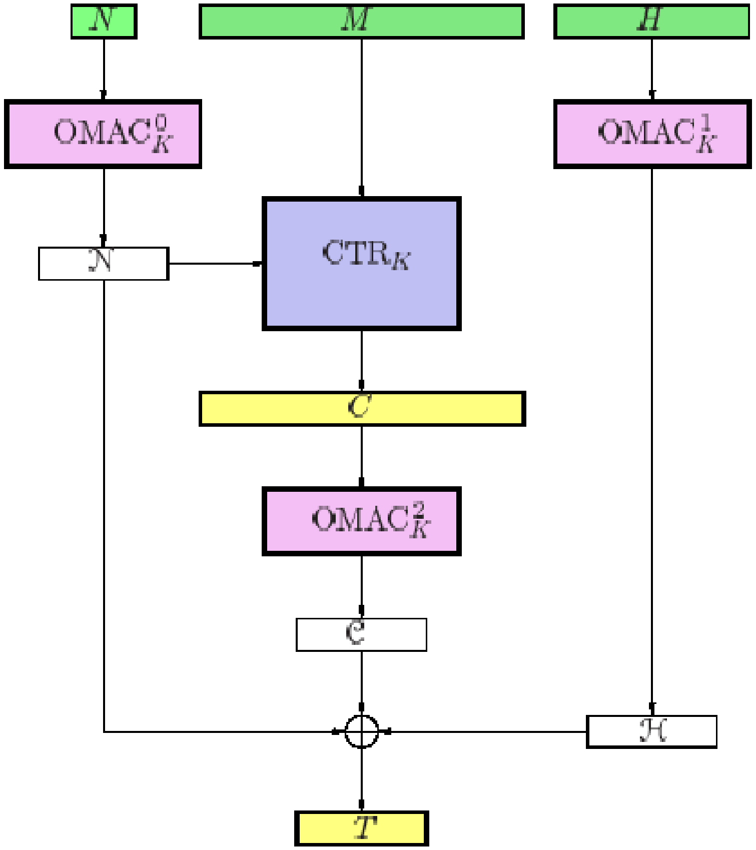
Source: [EAKD], Figure 2

The Modified counter mode of operation



Source: [SOBMO], Figure 3

The EAX mode of operation



Source: [EAX], Figure 3

References

Please refer to draft-bersani-eap-psk-01.txt available at:

- http://eappsk.chez.tiscali.fr/draft-bersani-eap-psk-01.txt
- http://www.arkko.com/publications/eap/draft-bersani-eap-psk-01.txt