MIKEY-TICKET

DRAFT-MATTSSON-MIKEY-TICKET-00

PRESENTER: ROLF BLOM

IETF 76, NOV 2009, HIROSHIMA
ORIGIN OF IDEA FOR MIKEY-TICKET

IMS media plane security (3GPP) for users requiring high security, e.g. enterprises and national security and public safety organizations.

Requirements
- Anchoring of trust/security external to IMS/SIP possible, i.e. trust/security is independent of trust/security in operator.
- Central policy control.
- Scalable and efficient.
- Group key management.
- Secure forking – late binding of keys to users.
- Remote-end user identity assurance.
- Pre-distribution of tickets.
- Support of deferred delivery.
The KMS resolves the ticket and modifies the keys, making them cryptographically unique for each responder targeted by forking.
MIKEY-TICKET

- Extends MIKEY with a set of new modes that uses a trusted KMS (Key Management Service) and a ticket concept, similar to Kerberos.
- MIKEY-TICKET consists of up to three roundtrips
  - Ticket Request, Ticket Transfer, Ticket Resolve
Ticket Request

- This exchange is used by the Initiator to request keys and a ticket from a trusted Key Management Service, with which the Initiator have a pre-established trust relation.

- The initiation message REQUEST_INIT comes in two variants corresponding to the pre-shared key (PSK) and public-key encryption (PK) methods of [RFC3830].

- TP is the desired ticket policy.

\[
\begin{align*}
\text{Initiator} & \quad \text{KMS} \\
\text{REQUEST_INIT_PSK} = & \quad \text{-----} \\
\text{HDR, T, RANDi, [IDRi],} & \quad \text{REQUEST_RESP =} \\
[\text{IDRkms}], \text{TP, [KEMAC]}, & \quad \text{HDR, T, [IDRkms],} \\
[\text{IDRpsk}], V & \quad \text{TICKET, KEMAC, V} \\
\text{REQUEST_INIT_PK} = & \quad \text{-----} \\
\text{HDR, T, RANDi, [IDRi], \{CERTi\},} & \quad \text{REQUEST_RESP =} \\
[\text{IDRkms}], \text{TP, [KEMAC]}, & \quad \text{HDR, T, [IDRkms],} \\
[\text{CHASH}], \text{PKE, SIGNi} & \quad \text{TICKET, KEMAC, V}
\end{align*}
\]
This exchange is used to transfer the ticket as well as session information from the Initiator to a Responder.

Similar to MIKEY-PSK but
- TICKET instead of KEMAC
- RANDi and RANDr gives mutual key freshness guarantee
- IDRr, RANDkms is used to modify keys, making them cryptographically unique for each responder targeted by the forking.

**Initiator**

```plaintext
TRANSFER_INIT =
HDR, T, RANDi, [IDRi], [IDRr],
{SP}, TICKET, V
```

**Responder**

```plaintext
< -- TRANSFER_RESP =
HDR, T, [RANDr],
[IDRr], [RANDkms], V
```
TICKET RESOLVE

› This exchange is used by the Responder to request the KMS to return the keys encoded in a ticket.
› The initiation message RESOLVE_INIT comes in two variants corresponding to the pre-shared key (PSK) and public-key encryption (PK) methods of [RFC3830].

Responder

RESOLVE_INIT_PSK =

HDR, T, RANDr, [IDRr],
[IDRkms], TICKET,
[IDRpsk], V

KMS

----->

RESOLVE_RESP

HDR, T, [IDRkms], KEMAC,
[IDRr], [RANDkms], V

----->

RESOLVE_INIT_PK =

HDR, T, RANDr, [IDRr], {CERTr},
[IDRkms], TICKET,
[CHASH], PKE, SIGNr

RESOLVE_RESP

HDR, T, [IDRkms], KEMAC,
[IDRr], [RANDkms], V
3 MAIN MODES OF OPERATION

**Full three roundtrip**
- Ticket generated by KMS
- Policy enforcement when ticket is generated
- Allows pre-distribution of tickets

**Kerberos like**
- Ticket generated by KMS
- Policy enforcement when ticket is generated
- Cannot handle secure forking/retargeting

**Otway-Rees like**
- Ticket generated by Initiator
- Policy enforcement when ticket is resolved
KEY FEATURES

› Trust is anchored in KMS, which can be independent of network operator.
› Allowed message exchanges and ticket options are determined by policy and can be adapted for different deployment scenarios: Policy enforcement is performed by the KMS.
› By defining groups of recipients, group key management becomes simple; 3GPP allows wildcarding for user group definitions. KMS verifies group membership.
› Secure forking and assurance of remote-end user identity
› “Reusable” tickets can be pre-distributed.
3GPP STATUS

› Specification is being finalized.
› MIKEY-TICKET based key management for high security applications.
› SDES based key management for other applications.