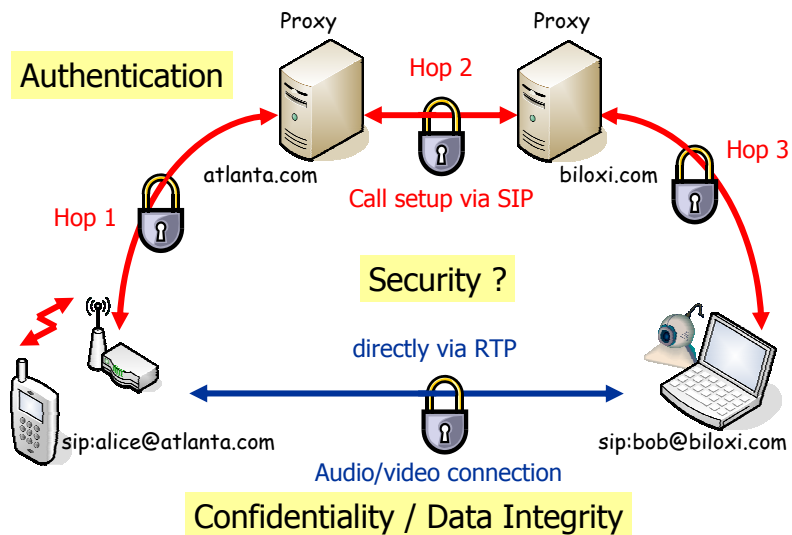


# Scalable Peer-to-Peer Security for SIP Clients

Prof. Dr. Andreas Steffen

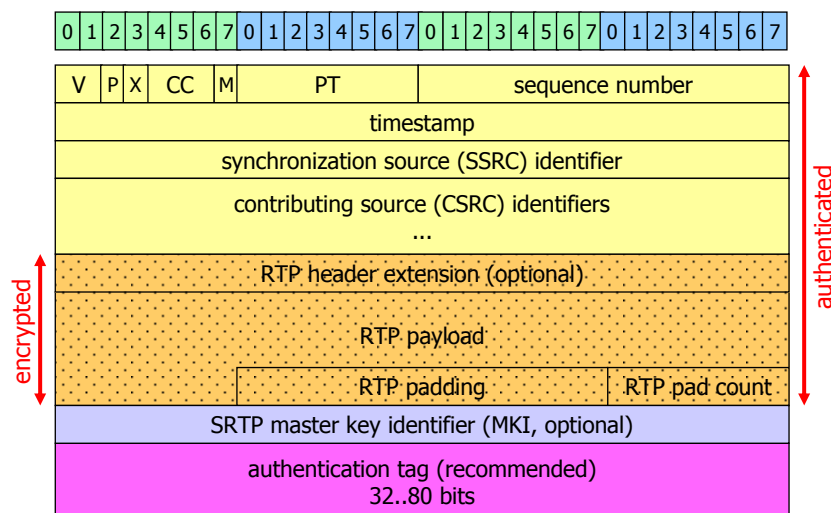
Institute of Internet Technologies and Applications  
Hochschule für Technik Rapperswil  
andreas.steffen@hsr.ch

## VoIP Communications Channels

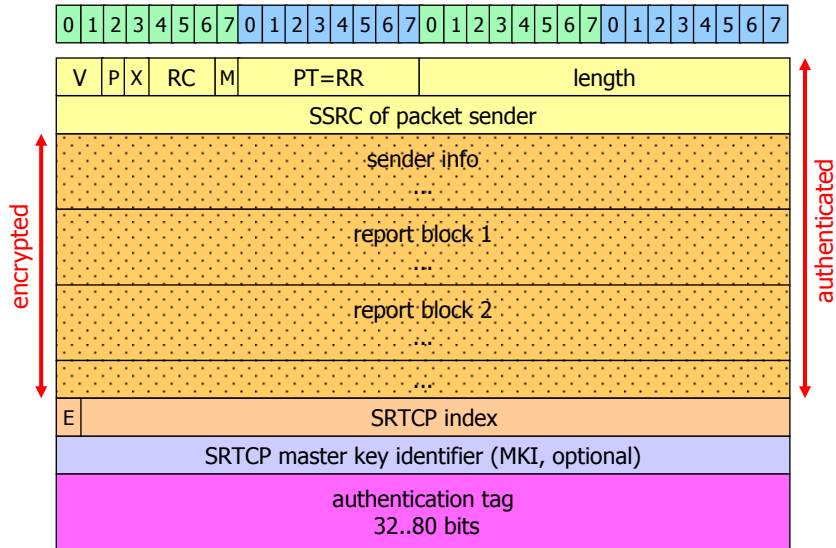


## Securing the Media Streams with Secure RTP

### Secure RTP Packet Format (RFC 3711)

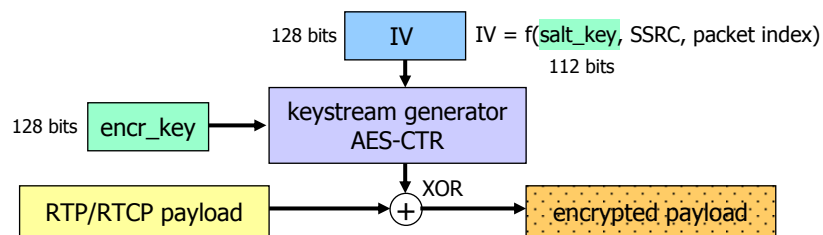


## Secure RTCP Packet Format (RFC 3711)

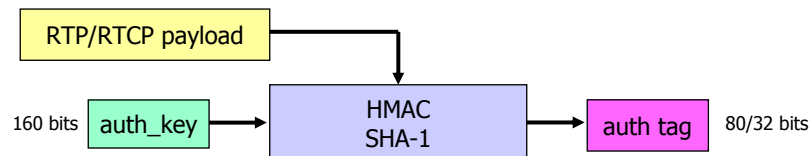


## Default Encryption and Authentication Algorithms

- Encryption uses AES in Counter Mode (AES-CTR) with 128 bit key

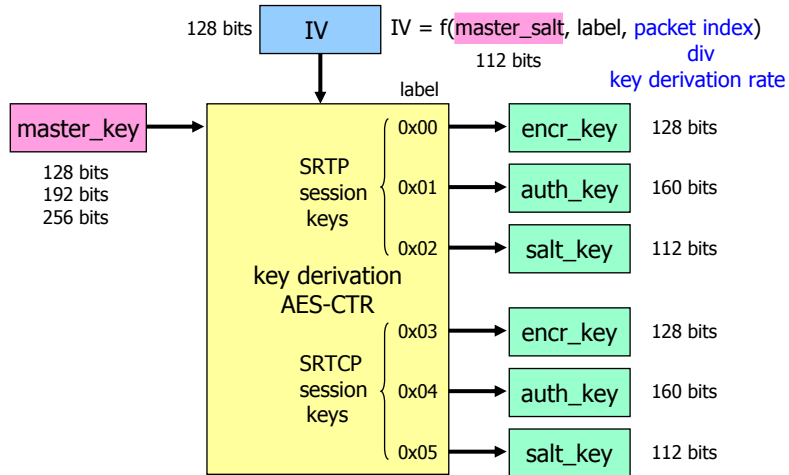


- Authentication uses HMAC-SHA-1 with truncated 80 bit MAC



## Session Key Derivation

- Key Derivation uses AES in Counter Mode (AES-CTR)



## Media Stream Encryption with Secure RTP

The screenshot shows the Kphone interface with SRTP settings. The 'Enable SRTP' checkbox is checked. The SRTP Master Key is displayed as '9kbFaZEIZFwJkMcIBi8TDiK:O4ML'. An outgoing call from sip:bob@biloxi.com is shown with status 'Ringing' and audio 'Attached (active)'. An incoming call from sip:alice@atlanta.com is shown with status 'Invitation received' and audio 'Unattached'. The 'Accept' button is highlighted. A media player window shows an audio file 'file:///root/voip/encrypted.au' with a duration of 00:02.

**SRTP for Kphone**  
Silvan Geser &  
Christian Höhn  
HSR Project 2005

**Problem:**  
How to distribute the  
SRTP Master Key?

## Securing the Media Streams

- Secure RTP
  - Needs a secret master key that must be distributed in a secure way.
  - The key exchange can be effected via the Session Description Protocol (SDP) payload that is transmitted during the SIP connection setup.
  - The SDP payload can be protected on a „hop-to-hop“ basis via **TLS** (i.e. SIPS). This approach allows „lawful inspection“ but on the down side requires full trust into the proxy-servers.
  - As an alternative the **Multimedia Internet KEYing** Protocol (MIKEY, RFC 3830) can be used which guarantees a true peer-to-peer key exchange. MIKEY payloads are also transported via SDP.
- IPsec
  - IPsec tunnels protecting media streams are set up via the **Internet Key Exchange** protocol (IKE). If there is already a site-to-site VPN or a remote access scheme in place then the VoIP calls can be transported via IPsec as well.
  - Drawback: Large IPsec overhead of 60-80 Bytes per RTP audio packet!

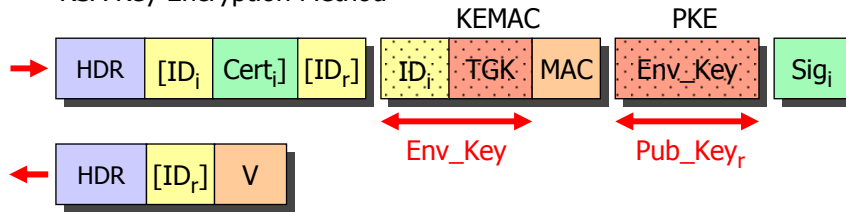
Telephony-Summit May 2 2006, Wiesbaden

## Secure Peer-to-Peer Key Exchange using MIKEY

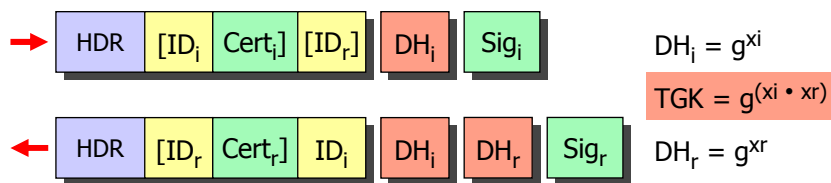
---

## MIKEY Key Exchange Methods

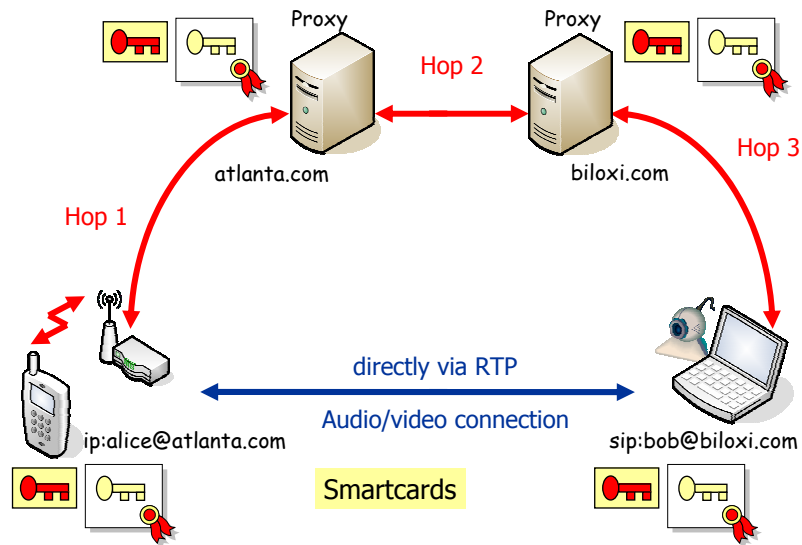
- RSA Key Encryption Method



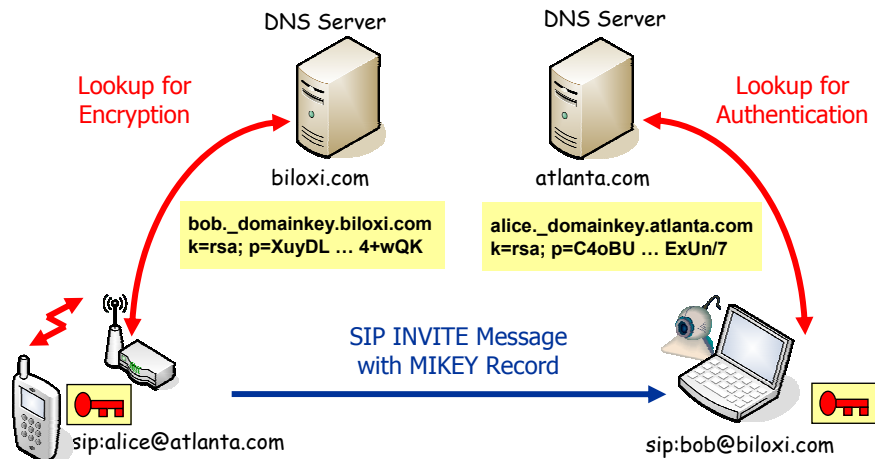
- Diffie-Hellman Key Exchange Method



## Dream or Nightmare? Strong PKI-based Security



## Pragmatical Approach: DomainKeys via DNS



HSR Diploma Thesis 2005 by Silvan Geser and Christian Höhn

## DomainKeys Generation

- `openssl genrsa -out myPrivateKey.pem 1024`
- `openssl rsa -in myPrivateKey -pubout -out myPublicKey`
- `cat myPublicKey`

```
-----BEGIN PUBLIC KEY-----  
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC114Y1oPxnYgrjKThuZVd1uJh2  
xMiP+wzPd0czDGpkw5w8Ex0ZGHnws1GfMIqSpCuzgR5SxEbJGkbD+lyeEbHhPs0T  
j37f3zar9LY3LTUCiTw7CfZHXAjC31VcSaeWrxEI+rjnPjUWjEAHycWOYqxs+dr  
fKt6gJJCz4UJZC3O9wIDAQAB  
-----END PUBLIC KEY----- k=rsa; p=MIGfMA0...wIDAQAB
```

- Public Key Cache folder stores DomainKeys in the OpenSSL format shown above:
  - `alice._domainkey.atlanta.com`
  - `bob._domainkey.biloxi.com`
  - `andreas.steffen._domainkey.hsr.ch`

## MIKEY Configuration in Kphone

Settings SRTP Socket Call Preferences Call Forwarding

Mode

Disabled  Pre-Shared Key (PSK)  Public-Key Encryption (PKE)

SRTP Master Key (length 30 characters):

f9kbFaZEtZxFwJkMcIBI8TD/KO4ML

PKCS#1 File Password:

PKCS#1 File Path:

/root/.kphone/private/myPrivateKey.pem

Public Key (retrieved from DNS) Cache Folder:

/root/.kphone/cache/

OK Cancel

## Summary

- **SRTP** - Confidentiality of VoIP Calls
  - The Secure RTP protocol (SRTP) offers efficient encryption and authentication of multi-media packets. The main problem is the secure distribution of the SRTP session keys.
- **MIKEY** – Secure Peer-to-Peer Key Exchange
  - The MIKEY protocol allows the secure key exchange between two or more peers. Two public key methods are defined: RSA key encryption (PKE) or Diffie-Hellman (DH). Both methods require the trusted distribution of the peers' public keys. The main problem is the lack of a global Public Key Infrastructure (PKI).
- **DomainKeys** – Global Public Key Distribution
  - The DNS-based DomainKeys scheme postulated by Yahoo et al. for trusted email can be used for the public key operations required by the MIKEY exchange. DNS requests are not very secure but in the future Secure DNS might be available.
  - DomainKeys fetching was realized by HSR students for Kphone and is currently being implemented for the minisip client.