3GPP TSG SA WG3 Security — S3#17 S3-010222

21 - 24 May, 2001

Phoenix, Arizona

Source: Ericsson

Title: Updated Work Item Description for Network based end-to end- security

Document for: Discussion & Action

Agenda Item:

Abstract: This is an updated work item description of Network Wide End to End Encryption of user traffic to 3G TS 33.102 'Security Architecture'. Change bars indicate the differences to the WI description as presented in S3-010090 in Gothenburg).

The basic idea is to introduce a key management scheme, which can be used to set up SA's between clients for SRTP and IPSec ESP. That is the only end-to-end encrypted services that are offered are IP based. These services are mainly the services carried by RTP in the IMS (Streaming , Voice, etc) and IP in the IMS (and possibly the PS domain). The new services will thus only affect the terminals and the IMS(/CN).

Work Item Description

Network-based end-to-end security

1 3GPP Work Area

~~X~~	Radio Access
X	Core Network
X	Services

2 Linked work items

There are five related work items in S3:
User plane protection in access network
Access security for IP-based services
Core network security: full solution
Lawful interception in the R00 architecture
Visibility and configurability

3 Justification

The R4~~00~~ system architecture ~~may create new requirements and/or opportunities for extending user plane traffic security further back into the core network. In addition it~~ may allow for security mechanisms to be

applied on an end-to-end basis, providing that the necessary lawful interception requirements are addressed when encryption is applied. This work will take advantage of concepts and hooks for key management for network-wide encryption which have been considered in R99.

4 Objective

The overall objective of this WI is to specify a network-based security architecture which provides security features to users on an end-to-end basis for IP based traffic (GPRS, VoIP, Streaming, etc). ~~The architecture is expected to be based on an evolution / re-use of the existing R99 security architecture~~.

The main security feature to be provided is expected to be encryption . However, the specification of other security features (e.g. authentication and integrity protection) will also be investigated.

The work ~~may~~ involves defining an appropriate key management architecture to support the end-to-end security mechanisms and the integration of these into the system architecture. Where possible this would be based on an evolution / re-use of the existing R99 authentication and key agreement mechanism. Some key management concepts for end-to-end security were presented in an old version of the R99 security architecture (33.102 v3.4.0).

The work may involve the specification of the end-to-end security mechanisms and the integration of these mechanisms into the system architecture. This work would involve the specification of an end-to-end security mode control mechanism which will handle algorithm selection, mode selection and user control. It would also involve the specification of any necessary end-to-end synchronisation mechanisms.

5 Service Aspects

Service requirements for end-to-end security need to be identified and addressed in conjunction with S1.

6 MMI-Aspects

Visibility and configurability of end-to-end security will be important. For example, the existing ciphering indicator may need to be enhanced to indicate whether or not the call is encrypted on an end-to-end basis.

7 Charging Aspects

End-to-end security may be considered to be a value-added service, especially if it is not, or cannot, be provided as a default.

8 Security Aspects

The main aspect of this work item is security.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes	X	X	~~X~~	X	
No					X
Don't know					

10 Expected Output and Time scale (to be updated at each plenary)

Meeting	Date	Activity

S3~#187	February 2001May 2001	Agreement of work item and CR to reintroduce text removed from R99
	April 2001	Definition of Work Tasks and completion of the plan for this Feature
S3#18	May 2001	Feasibility study and definition of security architecture: new CRs approved
S3#19	July 2001	Concept presented to CN, RAN, and T and GERAN
S3#20	October 2001	Integration of security architecture: Complete CRs
S3#21 and SA#14	December 2001	Integration of security architecture: CRs approved at TSG level

This table will be finalised when the plan for this feature is complete (see milestones above)

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102				
33.103				
33.105				

11 Work item raporteurs

Peter Howard
Communications Security and Advanced Development
Vodafone Ltd
The Courtyard
2-4 London Road
Newbury
RG14 1JX
Phone +44 1635 676206
Fax +44 1635 231721
peter.howard@vf.vodafone.co.uk

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Draft list: Vodafone, BT, Nortel, Lucent

14 Classification of the WI (if known)

(X)	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

SRTP

- Secure Real Time Transport Protocol -

Joint work with:
{Blom, Carrara, Norrman, Näslund} @ Ericsson
{McGrew, Oran} @ Cisco

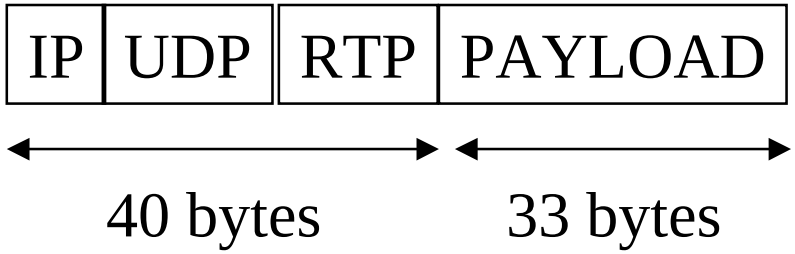
Overview

- Requirements on VoIP and Streaming security in wireless setting
- Development of SRTP
- SRTP description
- Open issues

Background: VoIPoW

Speech coder produces 33 byte data every 20ms

Sent over RTP/UDP/IP



Bandwidth problem!

Header Field Classification

INFERRED These fields contain values that can be inferred from other values. Need not be sent at all.

E.g. RTP timestamp (typically)

STATIC These fields are expected to be constant throughout the lifetime of the packet stream. Need to be communicated once.

E.g. IP version

KNOWN Expected to have well-known values and therefore do not need to be communicated at all.

E.g. IP header length

CHANGING These fields are expected to vary in some way: randomly, within a limited value set or range, or in some other manner.

E.g. UDP checksum

ROHC

RObust Header Compression:

on average reduces 40 byte header to 1 byte!

(recent IETF RFC)

Background on RTP

- Described in RFC1889
- Security vague and not appropriate. Status:
  - network/transport security (IPsec, TLS)
  - application security
- Contributions requested by the AVT chairmen at IETF 48th

Requirements on RTP Encr.

1. low computational cost, speed
2. low footprint
3. limited packet expansion — Stream cipher
4. no error propagation — Stream cipher
5. “fast-forward/rewind” in cryptostream — Blockcipher based
6. header compression compatibility
7. independence of transport layer
8. multiple RTP sessions sharing keys
9. secure — AES-based

Requirements on RTP Auth.

Two main problems:

- bandwidth consumption (MAC adds > 10%)
- even using a very short MAC (with lower security), still a given speech quality requirement is

  'no dropped packets due to bit errors in the payload'

- UEP & UDP Lite

authentication has a cost in cellular environments

49th IETF Meeting, Dec 2000

Ericsson contributions:

VoIPoW-driven

Confidentiality of media streams

Goal: to end up with a service as ***attractive*** as today's CS (***cost*** and ***speech quality***)

requirements- and solution draft presented

49th IETF Meeting (2)

Cisco contribution

- military applications
- one draft presented at IETF 49th

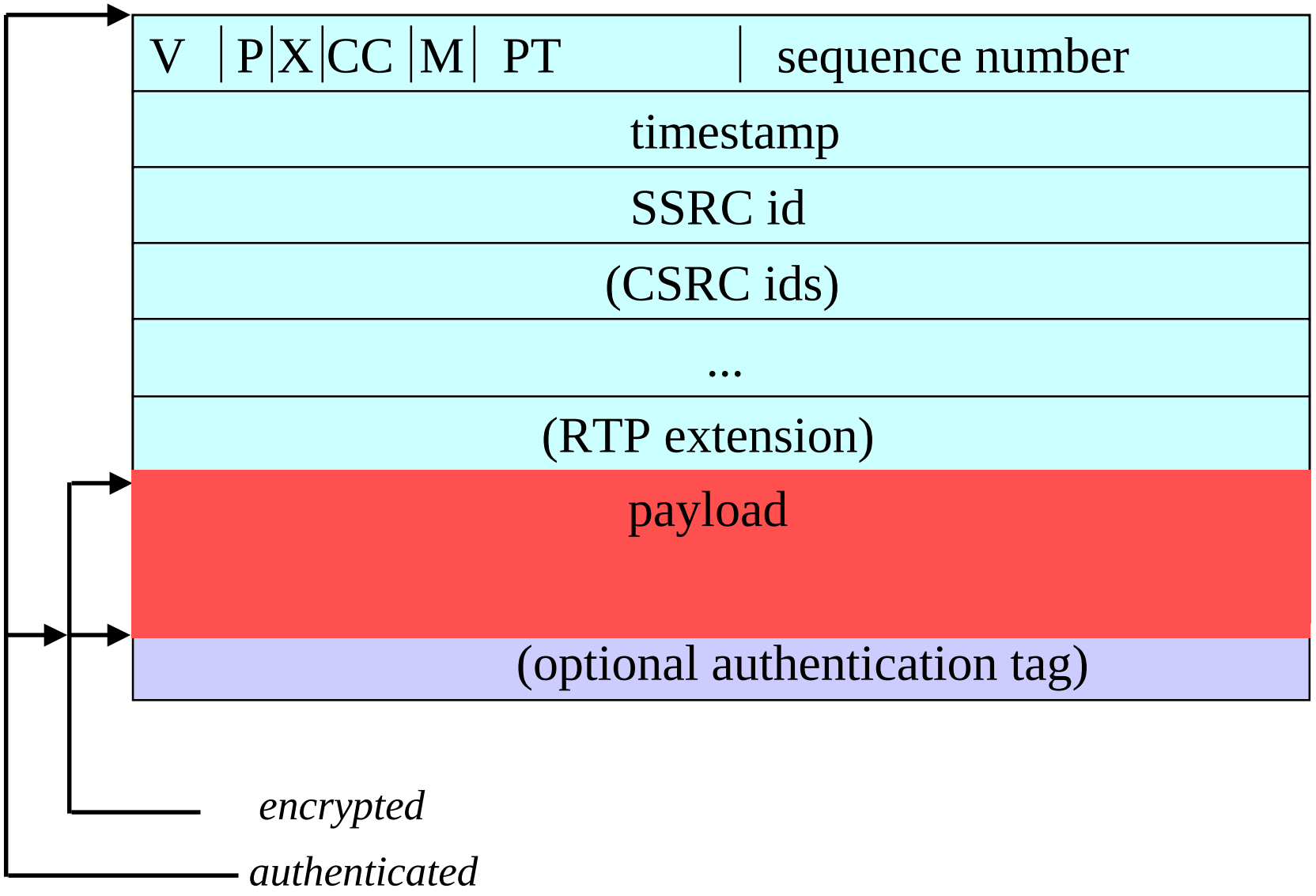
SRTP is Born...

- IETF draft, Ericsson/Cisco merge
- a WG item for AVT
- presented at the 50th IETF, March 2001

SRTP

- RTP profile
- Objectives:
  - confidentiality of RTP payload (not headers)
  - authentication of RTP packet
  - anti-replay protection
  - implicit RTP header authentication

SRTP packet


V
P
X
CC
M
PT
sequence number
timestamp
SSRC id
(CSRC ids)
...
(RTP extension)
payload
(optional authentication tag)
encrypted
authenticated

SRTP Crypto Context

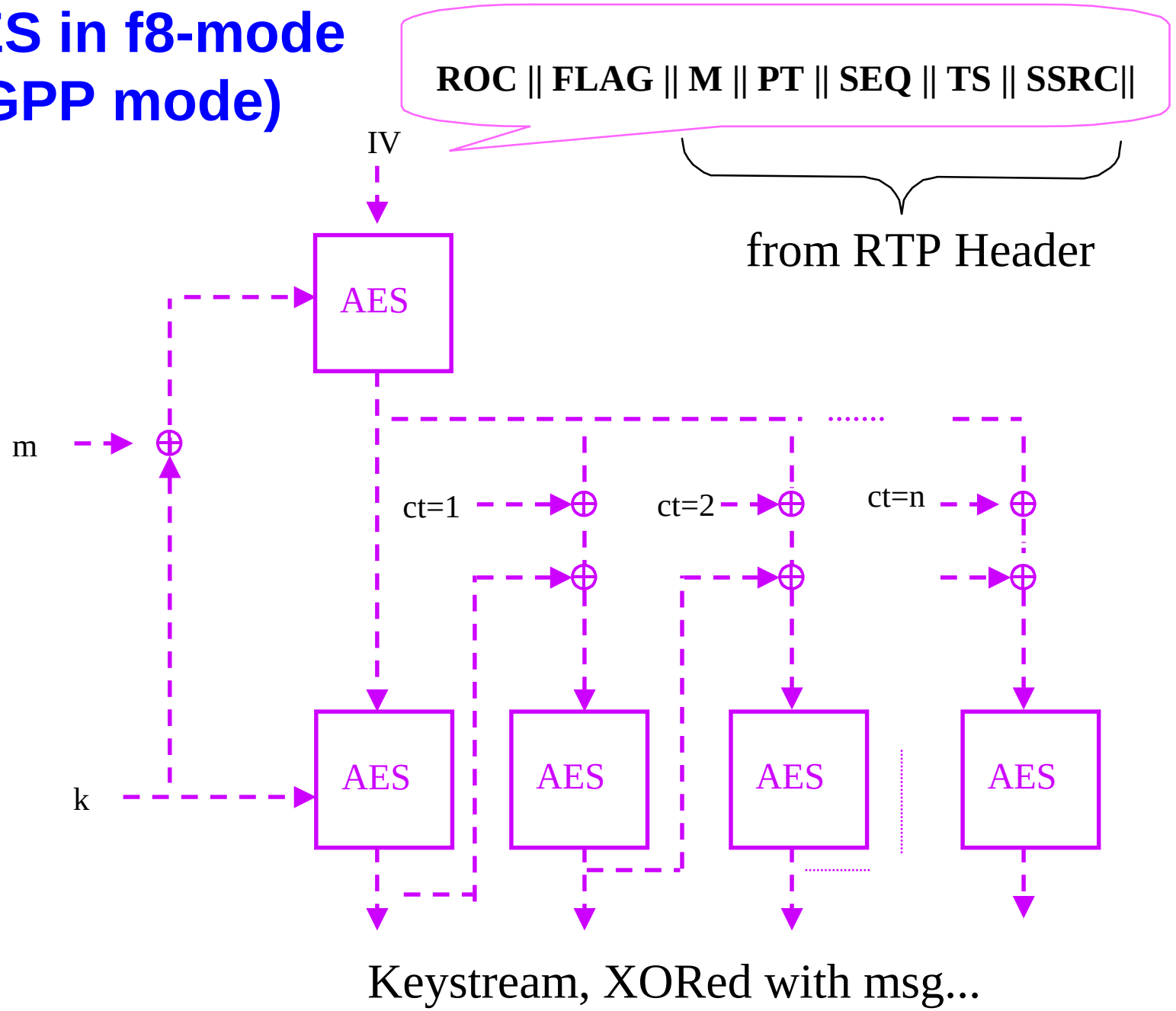
- keys (cipher + auth)
- 32-bit rollover counter
- FLAG (distinguishes RTP/RTCP)
- mode of operation for block cipher
- (authenticated) sequence number
- replay list

SRTP Crypto Suite

- **Mode for block cipher**
  - Segmented Counter Mode, or,
  - f8
- **Cipher**
  - AES/128
- **(Optional) Authentication**
  - UMAC16
- **Sync:** implicit index

- **Speed** [PIII 600] Encryption: 106Mb/s
  Auth: 7500000 rej/s

AES in f8-mode (3GPP mode)



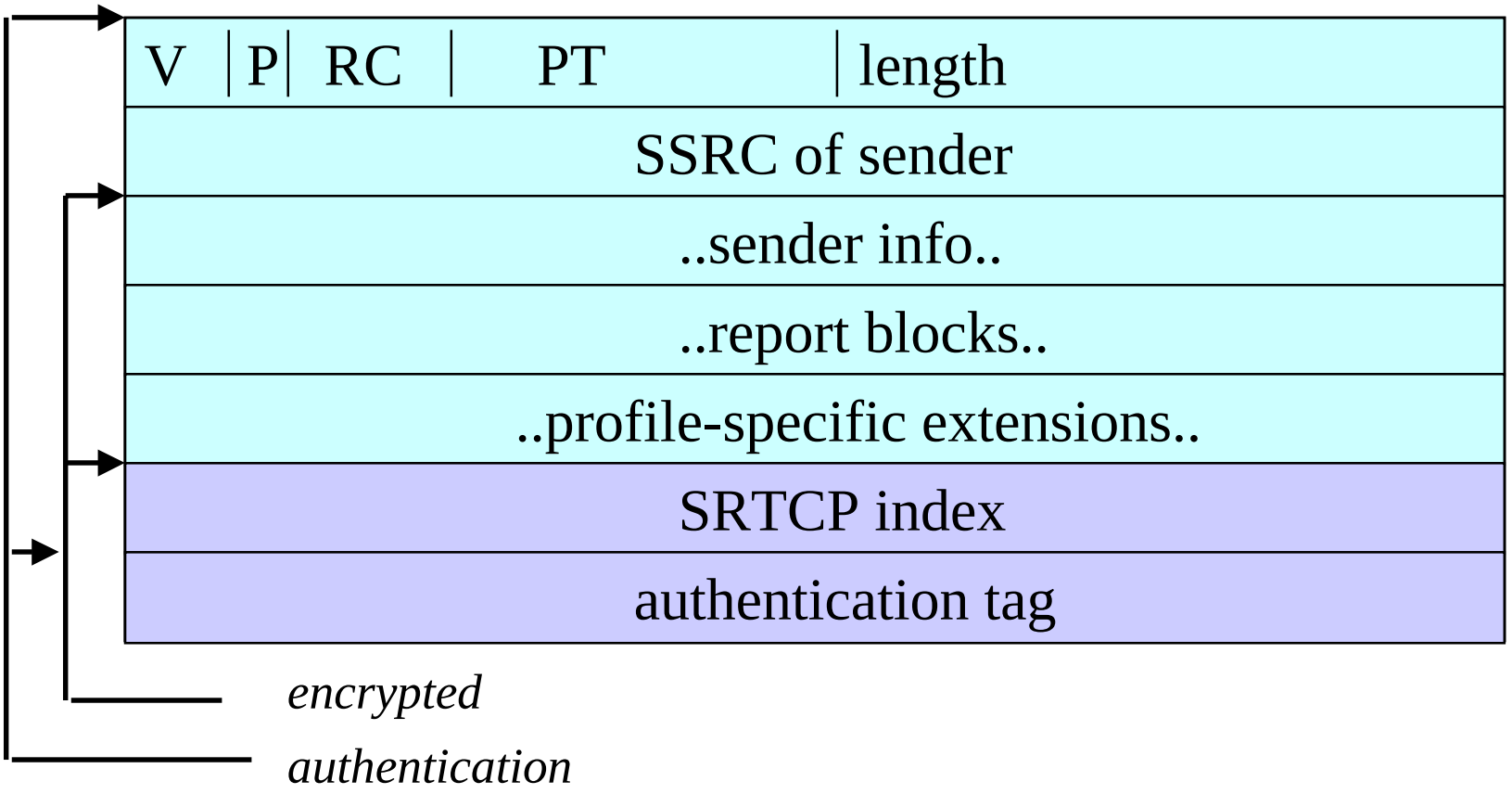
IPsec Applicability

IPsec is *the* promising security solution for the All-IP scenario

and ROHC supports IPsec HC ***but***

- ‘transport ESP’
  - the most efficient ROHC profile does not work
  - IPsec header
- ‘tunnel ESP’
  - header overhead
- AH and ESP+auth
  - bandwidth and cost

SRTCP



- mandatory authentication
- allows split into encrypted /unencrypted “packethalves” (3rd party monitoring)

Open Issue

Key Management

51th IETF, London, August 2001

- v .01 of SRTP draft
  - scenarios, parameters from the key mgt, SDP, SSRC vs keys, and some fixing
- WG Last Call after London??