ITU-T Workshop
IPCablecom - Mediacom 2004
Session 2 - Security & Privacy

13 March 2002, Geneva/CH

SIEMENS

Information
and Communication
Networks

Dipl.-Inform. Martin Euchner
Rapporteur Q.G/16
Siemens AG, Information & Communication Networks, M SR 3
81359 Munich, Germany
Tel: +49 89 722 55790 E-mail: martin.euchner@icn.siemens.de

Multimedia Security within Study Group 16
Past, Presence and Future

Outline of Presentation

- Study Group 16 Overview
  - Question G “Multimedia Security”
- Examples of past, present and future MM-security in SG16
  - Secure H.323-based IP Telephony
  - H.235 and associated security profiles
  - H.248 Media Gateway Decomposition Security
  - Secure H.320 Audio/Video and T.120 Data Conferencing
  - Emergency Telecommunications Services Security

Part I

ITU-T Study Group 16

Question G “Security of MM Systems & Services“

Study Group 16 - Security-related Questions in the MediaCom2004 project

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

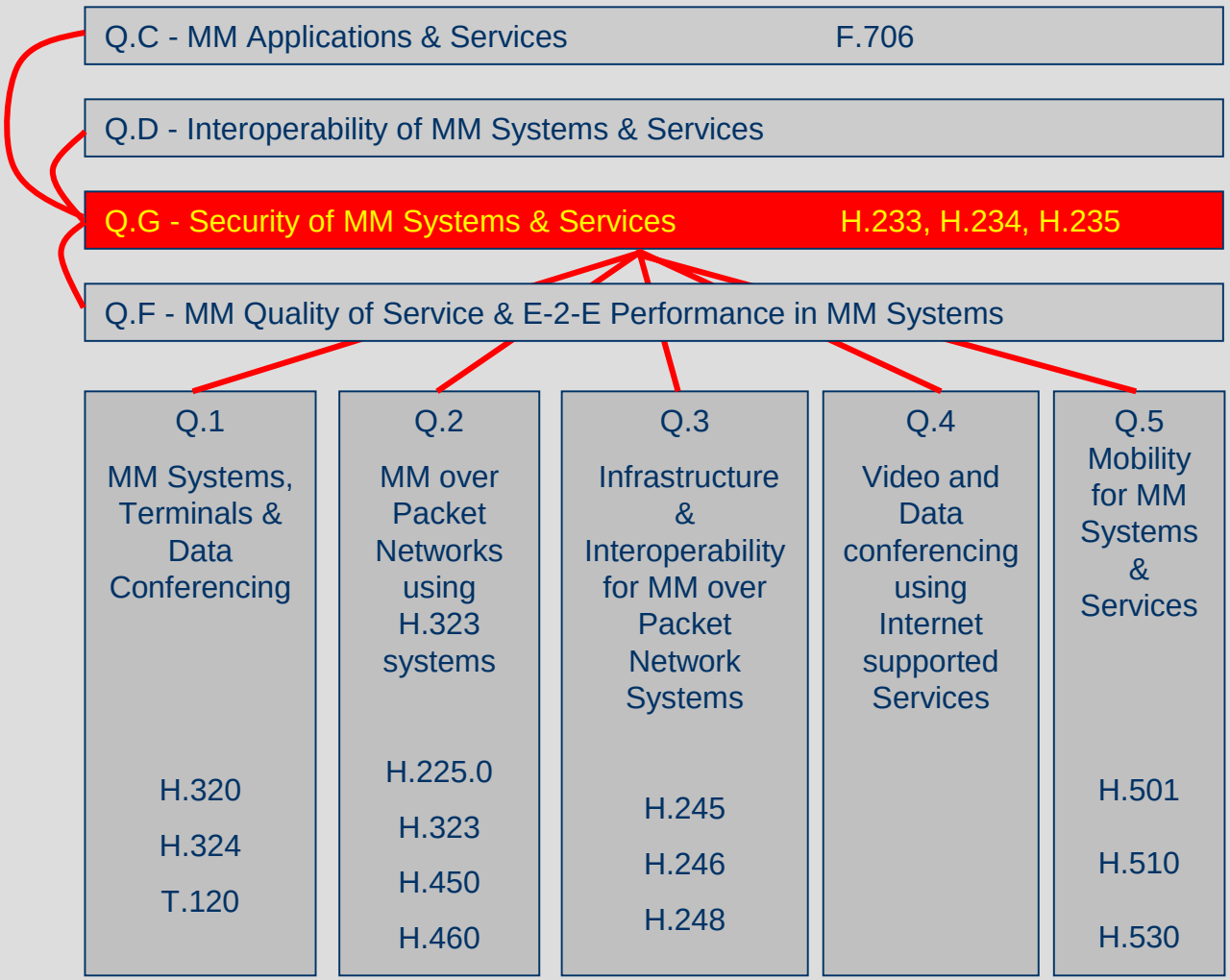
H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS



Question G
Security of MM Systems & Services

SG16 & Q.G ⇐

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS

- A horizontal question with broad focus
- General Responsibilities:
  - Perform threat analysis, analyze security requirements; recommend security services/mechanism for MM applications
  - Build sound security architecture and interface with security infrastructure
  - Realize multimedia communications security, engineer MM security protocols with real-time, group-communication, mobility and scalability constraints
  - Address interdomain security and security interworking
  - Maintain H.233, H.234; progress H.235

For further details on Q.G terms of reference, please see Annex G of the Mediacom2004 project description

http://www.itu.int/ITU-T/studygroups/com16/mediacom2004/index.html

Multimedia Communications Security
Some questions to address

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS

- Secure the signaling for MM applications
- Secure data transport and MM streams
- Protect MM content (authorship, IPR, copy-protection)
- Efficiently integrate key management into MM protocols; interface with security infrastructures (e.g., PKI)
- Negotiate security capabilities securely
- Interact with security gateways and firewalls
- Enable MM security across heterogeneous networks
- Provide scalable security
  (small groups, medium sized enterprises, large carrier environments)
- Build future-proof security
  (simple and sophisticated security techniques)
- Address the performance and system constraints (SW/HW crypto, smart-cards,...)
- ….

Q.G Work and Study Items
Some Highlights

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS

- Investigate confidentiality and privacy of all signaling
- Address the concept of a centralized key management for MM systems
- Security for MM Mobility, MM Presence, MM Instant Messaging
- Optimize voice encryption, develop video encryption, consider sophisticated crypto algorithms
- MM security support for emergency services
- Consolidate or develop new security profiles
- Clarify the impact due to lawful interception
- Architect secure, de-composed systems
- Security interworking H.323-SIP
- Interaction with e-commerce and network security
- ...

Target Multimedia Applications with Security Needs

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

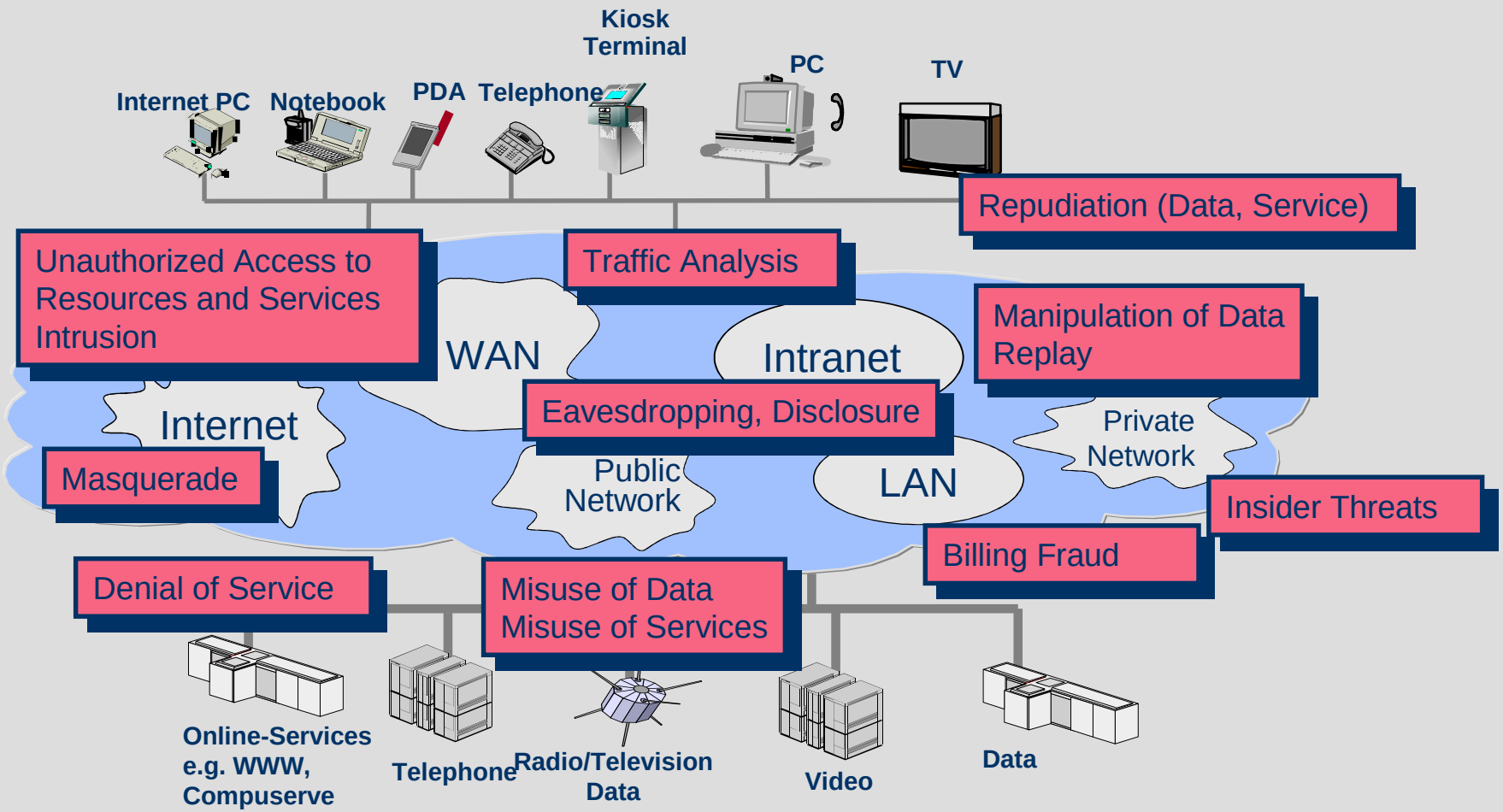
H.248 Security

Secure A/V & Data Conferencing

Secure ETS

- Voice/Video Conferencing
- Data Conferencing
- IP Telephony (Voice over IP)
- Media Gateway Decomposition
- Instant Messaging and MM-Presence

Threats to Multimedia Communication

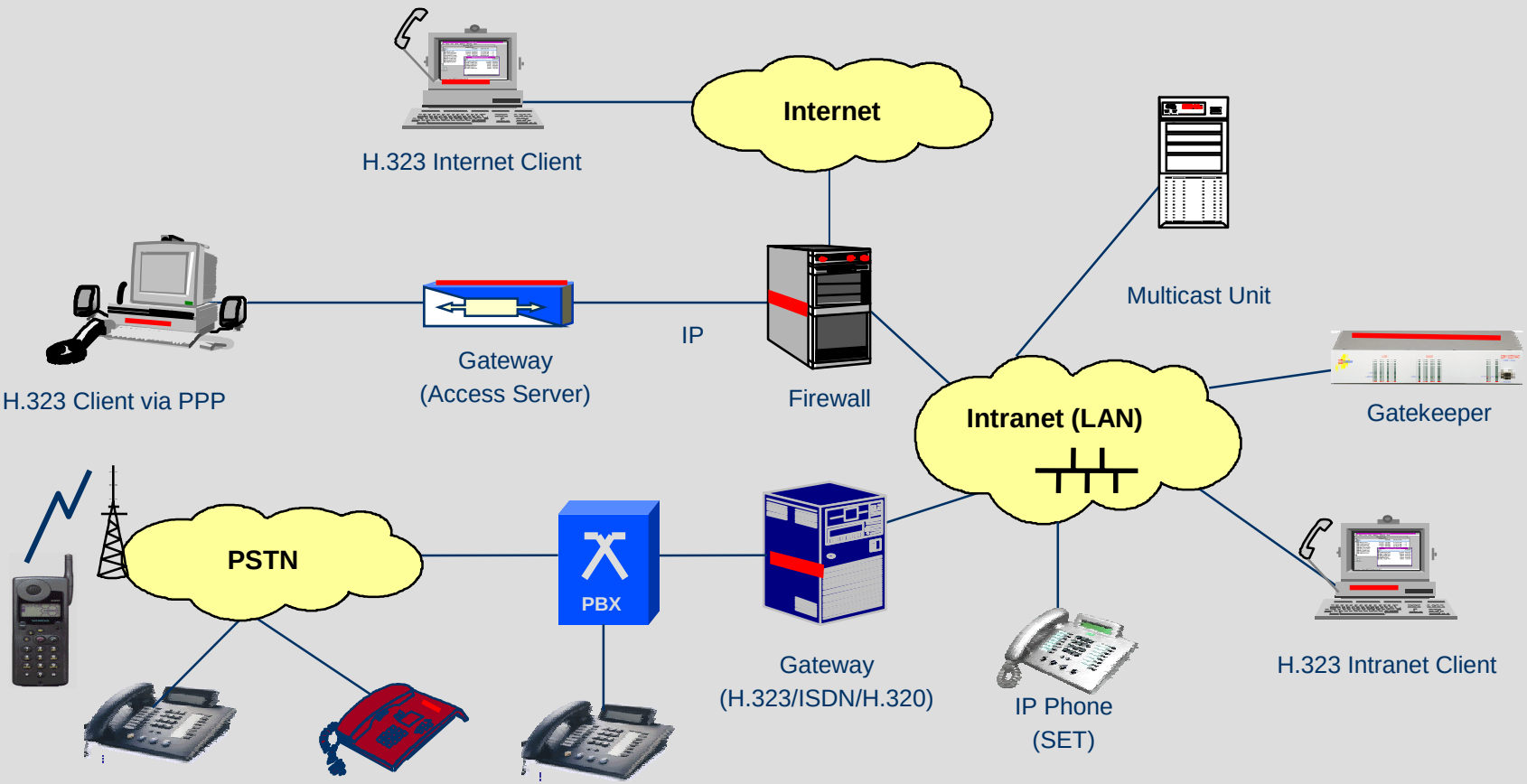


Part II

Secure IP Telephony

H.235
H.235 Annex D
H.235 Annex E
H.235 Annex F
H.235 Version 3
H.530

General H.323 Scenario



IP Telephony - Security Issues

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS

- User authentication:
  - Who is using the service? (Who am I phoning with?)
- Call authorization:
  - Is the user/terminal permitted to use the service resources?
- Terminal and server authentication:
  - Am I talking with the proper server, MCU, provider? Mobility ...
- Signaling security protection;
  - Protection of signaling protocols against manipulation, misuse, confidentiality & privacy
- Voice confidentiality:
  - Encryption of the RTP voice payload
- Key management:
  - Secure key distribution and key management among the parties
- Interdomain security:
  - Security profile & capability negotiation, firewall traversal

Specific IP Telephony Security Challenges

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS

- IP Telephony is real-time, point-2-point or multi-point
  - secure fast setup/connect
  - real-time security processing of media data
  - real-time certificate processing
  - IKE security handshakes take too long
- Security measures must be integrated in proprietary platforms and in VoIP stacks
  - security can best be added at application layer
  - tight interaction with voice CODECs and DSPs
  - low overhead for security: small code size, high performance,...
  - “Windows 5000” is not the answer!
- Secure management of the systems
  - secure password update
  - secure storage in databases
- Scalable security from small enterprise to large Telco environments
- Security should be firewall friendly

"Historic" Evolution of H.235

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

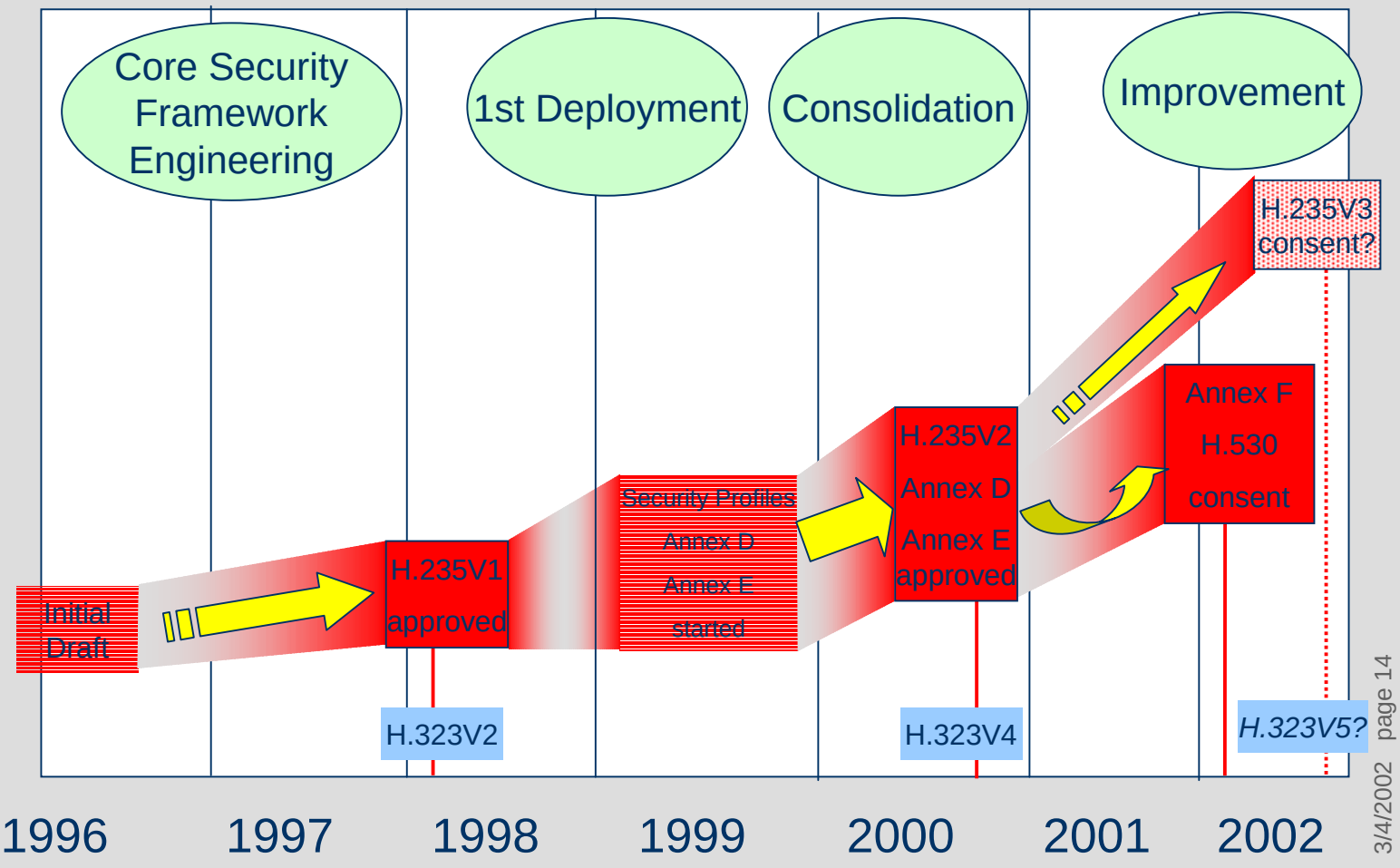
H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS



H.235 – Security for H.323

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

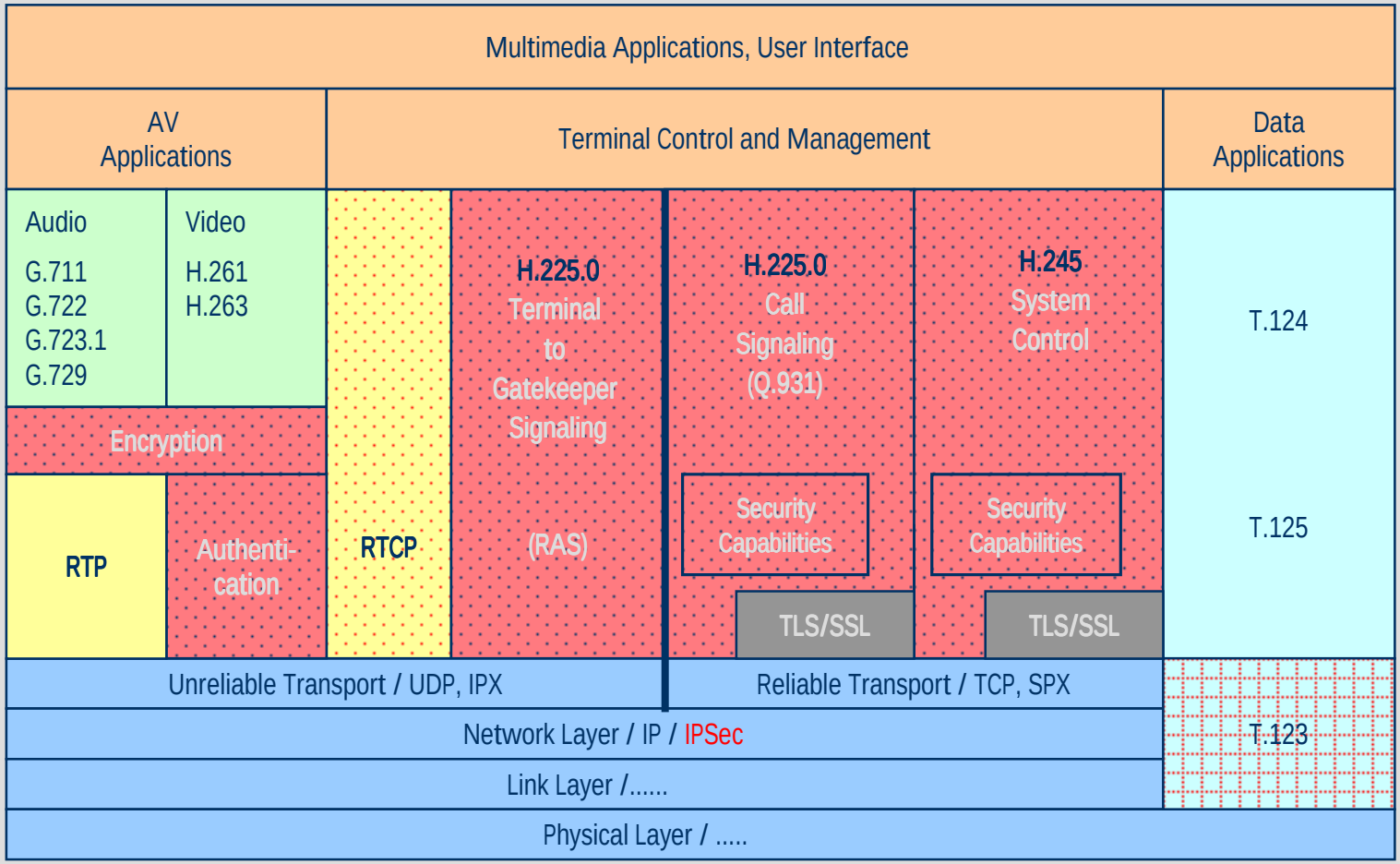
Secure A/V & Data Conferencing

Secure ETS

"Security and Encryption for H.323 and other H.245-based multimedia terminals"

- provides cryptographic protection of control protocols (RAS, H.225.0 and H.245) and audio/video media stream data
- negotiation of cryptographic services, algorithms and capabilities
- integrated key management functions / secure point-to-point and multipoint communications
- interoperable security profiles
- sophisticated security techniques (Elliptic curves, anti-spamming & AES)
- may use existing Internet security packages and standards (IPSec, SSL/TLS)
- Recommendation H.235 version 2 released in 11/2000

H.235 - "H.323 Security" Security Protocol Architecture



H.323 Phases with H.235 Security

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS

H.323 Phases

H.225.0 RAS	1.) GK Discovery 2.) Endpoint Registration 3.) Admission and Bandwidth request 4.) Establish Q.931 address	• Endpoint identification with DH-key exchange • Endpoint authentication (replay protected pw/certificate) • Access control and call authorization with access tokens • RAS message integrity, replay protection • ...
H.225.0 CS	1.) Call remote endpoint by Q.931 2.) Establish H.245 address	• Security port signaling and SSL/TLS secured call signaling • Negotiation of H.245 security channel capabilities • Secured fast connect with key management • ...
H.245 CC	1.) Open Control Channel 2.) Negotiate terminal capabilities 3.) Determine Master/Slave relationship 4.) Establish UDP ports for A/V 5.) Open/close logical channels	• SSL/TLS secured H.245 stack • Tunneling via H.225.0 CS Facility Messages • Terminal security capability negotiation • Integrated key management (pairwise/multipoint keys) • ...
H.225.0 Media	1.) Transfer Audio or Video Data within logical channel using RTP	• Audio/Video payload encryption

H.235 Profiles

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS

Goal: Select useful, interoperable set of security features of H.235

- H.235v2:
  - Baseline Security Profile for Authentication & Integrity with shared secrets
  - Signature Security Profile for Authentication/Integrity with certificates and digital signatures
  - Voice Encryption Security Profile for confidentiality with voice encryption
- H.235 Annex F:
  - Hybrid Security Profile
- H.530:
  - H.235 Mobility Security for H.510
- H.323 Annex J:
  - Baseline Security Profile for Simple Endpoint Types

H.235 Annex D
Baseline Security Profile Background

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

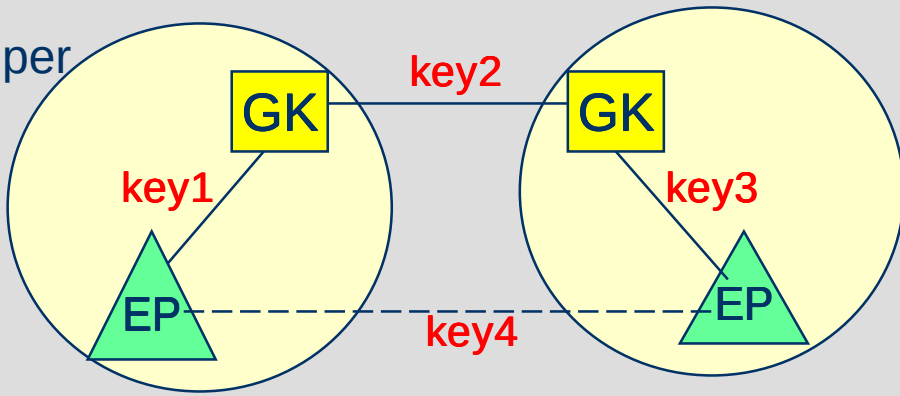
H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS

- Relies on symmetric techniques (shared secrets, passwords)
- Supported scenarios:
  - endpoint to gatekeeper
  - gatekeeper to gatekeeper
  - (endpoint to endpoint)



- Favors GK routed signaling with hop-by-hop security, (direct call model possible but limited)
- Supports secure fast connect with secure H.245 tunneling

H.235 Annex D
Baseline Security Profile

Security Services	Call Functions			
	RAS	**H.225.0**	**H.245(*)**	**RTP**
Authentication	Password HMAC-SHA1-96	Password HMAC-SHA1-96	Password HMAC-SHA1-96	
Non-Repudiation				
Integrity	Password HMAC-SHA1-96	Password HMAC-SHA1-96	Password HMAC-SHA1-96	
Confidentiality				
Key Management	Subscription-based password assignment	Subscription-based password assignment		

(*) H.245 tunneling, fast connect

H.235 Annex D Security Profiles
Countered Threats

SG16 & Q.G

Secure IP Telephony

H.235
Annex D
Annex E
Annex F
H.235 V3
H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS

Threats and attacks	Countermeasures
Masquerading, man-in-the-middle	Cryptographic authentication
Spoofing, connection hijacking	Authentication, integrity
Replay	Timestamp, sequence number
Message manipulation	Message digest
Denial-of-service	Message digest
Interception of media stream data	Symmetric encryption

H.235 Annex D
Voice Encryption Profile

Security Services	Call Functions						
	RAS	H.225.0	H.245	RTP			
Authentication							
Non-Repudiation							
Integrity							
Confidentiality				56-bit DES	56-bit RC2-com-patible	168-bit Triple-DES	*128-bit AES*
Key Management		authenticated Diffie-Hellman key-exchange	Integrated H.235 session key manage-ment (key distri-bution, key update using 56-bit DES/ 56-bit RC2-compatible/ 168-bit Triple-DES)/ *128-bit AES*				

H.235 Annex D
Voice Encryption - Background

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS

- Supports media encryption (RTP payload) end-to-end
- Allows different crypto algorithms and modes
- Allows different key management options
- Tight interaction of encryption function with media codec/DSP possible
- RTP header remains in clear supporting IP/UDP/RTP header compression
- Crypto algorithms, modes and parameters are negotiated by H.245 signaling.

H.235 Media Encryption

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

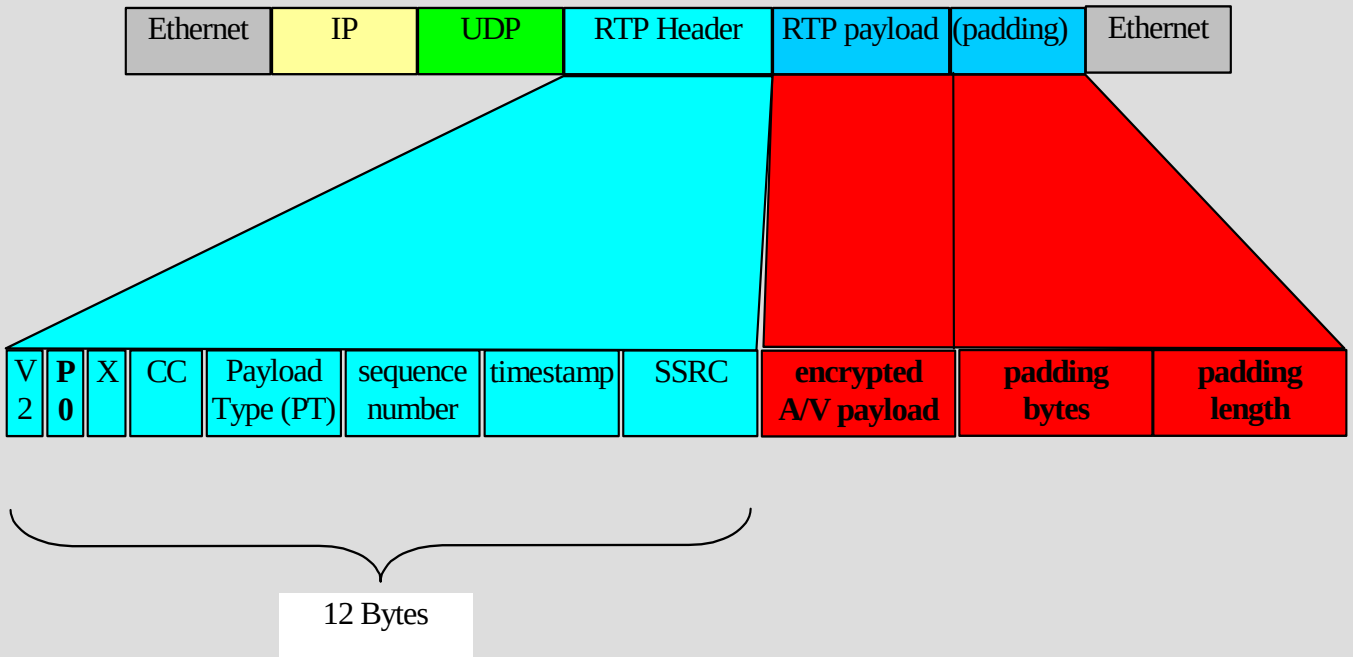
H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS



H.235 Annex E
Signature Security Profile

Security Services	Call Functions			
	RAS	H.225.0	H.245	RTP
Authentication	SHA1/ MD5	SHA1/ MD5	SHA1/ MD5	
	digital signature	digital signature	digital signature	
Non-Repudiation	SHA1/ MD5	SHA1/ MD5	SHA1/ MD5	
	digital signature	digital signature	digital signature	
Integrity	SHA1/ MD5	SHA1/ MD5	SHA1/ MD5	
	digital signature	digital signature	digital signature	
Confidentiality				
Key Management	certificate allocation	certificate allocation		

H.235 Annex E
Signature Security Profile - Background

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS

- Relies on asymmetric techniques (digital certificates, public/private keys)
- Supports proxy Gatekeeper (security proxy)
- GK routed signaling and direct call model possible
- Scalable for large, global environments
- Supports non-repudiation and secure fast connect
- Hop-by-hop and end-to-end security possible
- Optional voice-encryption

H.235 Annex F
Hybrid Security Profile

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

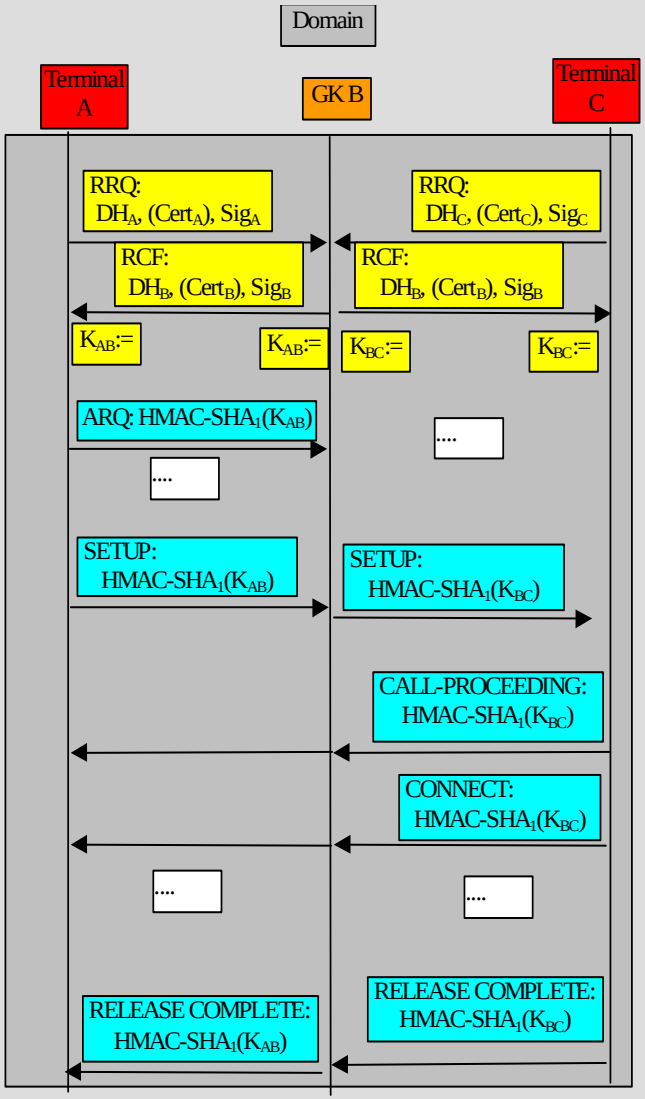
Secure A/V & Data Conferencing

Secure ETS

- Combines symmetric with asymmetric techniques
  - Baseline Security Profile with symmetric cryptography (H.235 Annex D)
  - Signature Security Profile with asymmetric cryptography (H.235 Annex E)
- Provides performance optimized global security
- Interoperates with PKI-based e-commerce environments

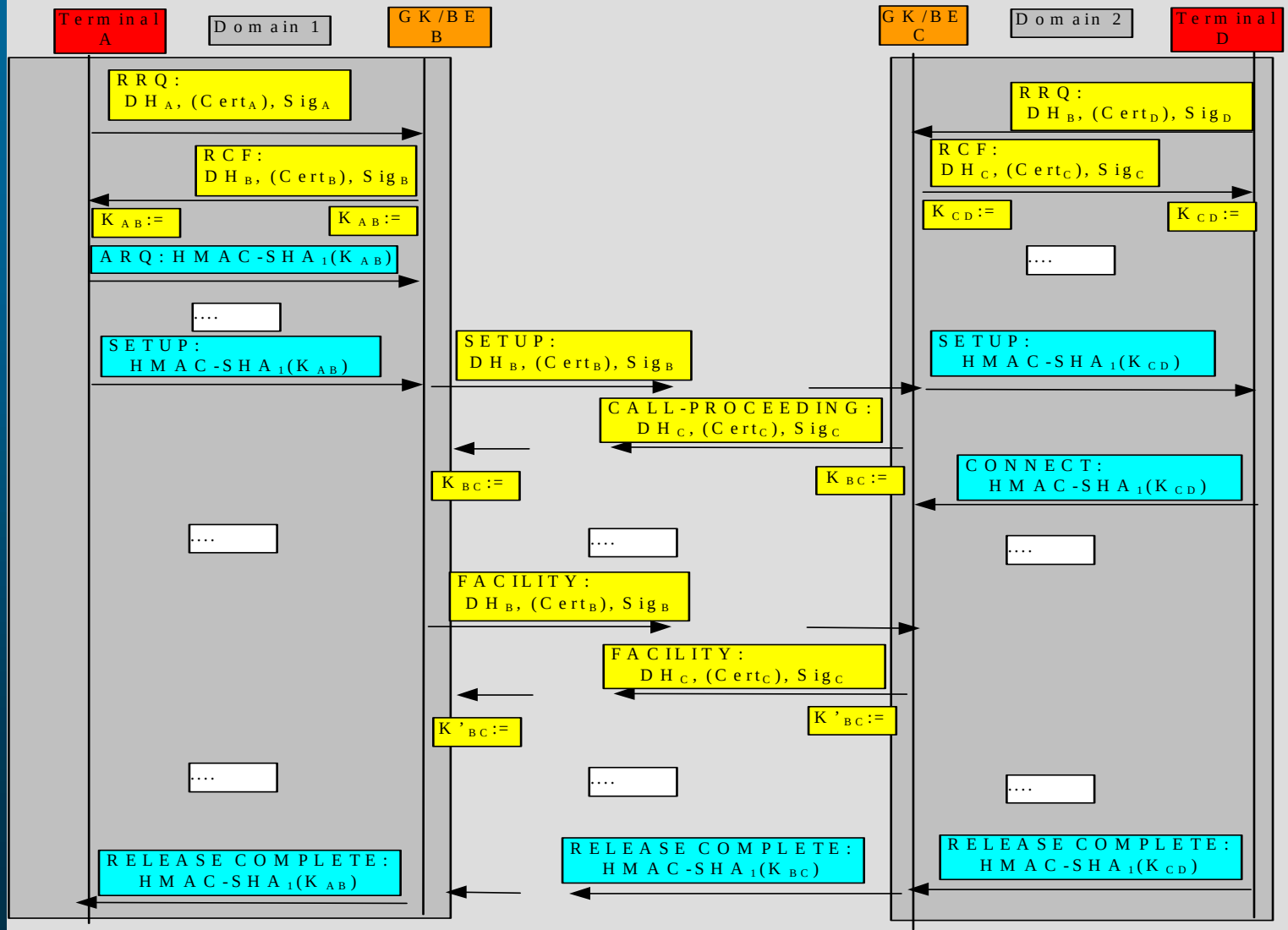
  ⇒ Voice-commerce
- Proposal by TEN Telecom Tiphon (TTT)/VISIONng Project: Security will be implemented for carrier VoIP field trial

H.235 Annex F
Hybrid Security Profile



- Asymmetric PKI crypto operations occur only at initial RAS registration
- Digital signature and certificate exchange for “secure RAS registration”
- Negotiated Diffie-Hellman key acts as a dynamic shared secret (replaces the static password)
- Any further RAS, Call signaling and Call Control efficiently secured by symmetric crypto operations
- Works also between Domains
- Includes re-keying and allows channel bundling

H.235 Annex F
Interdomain Scenario



H.235 Annex F
Hybrid Security Profile

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS

Security Services	Call Functions			
	RAS	H.225.0	H.245	RTP
Authentication	RSA digital signature (SHA1)	RSA digital signature (SHA1)	RSA digital signature (SHA1)	
	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	
Non-Repudiation				
Integrity	RSA digital signature (SHA1)	RSA digital signature (SHA1)	RSA digital signature (SHA1)	
	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	
Confidentiality				
Key Management	certificate allocation,	certificate allocation,		
	authenticated Diffie-Hellman key-exchange	authenticated Diffie-Hellman key-exchange		

H.235 Version 3
Work Items under Consideration

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS

- Deploying the Advanced Encryption Algorithm (AES) ✓
- Improved and more secure generation of the initial value (IV)
- Interworking with Secure Realtime Transport Protocol (IETF SRTP) and secure RTCP
- IETF MIKEY real-time key management consideration and interworking
- J.170 interworking
- Secure DTMF transport within H.245
- Signaling encryption with H.460.1 (Generic extensibility framework)
- Security for Emergency Telecommunications Services

H.530
The Security Problem of H.323 Mobility

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

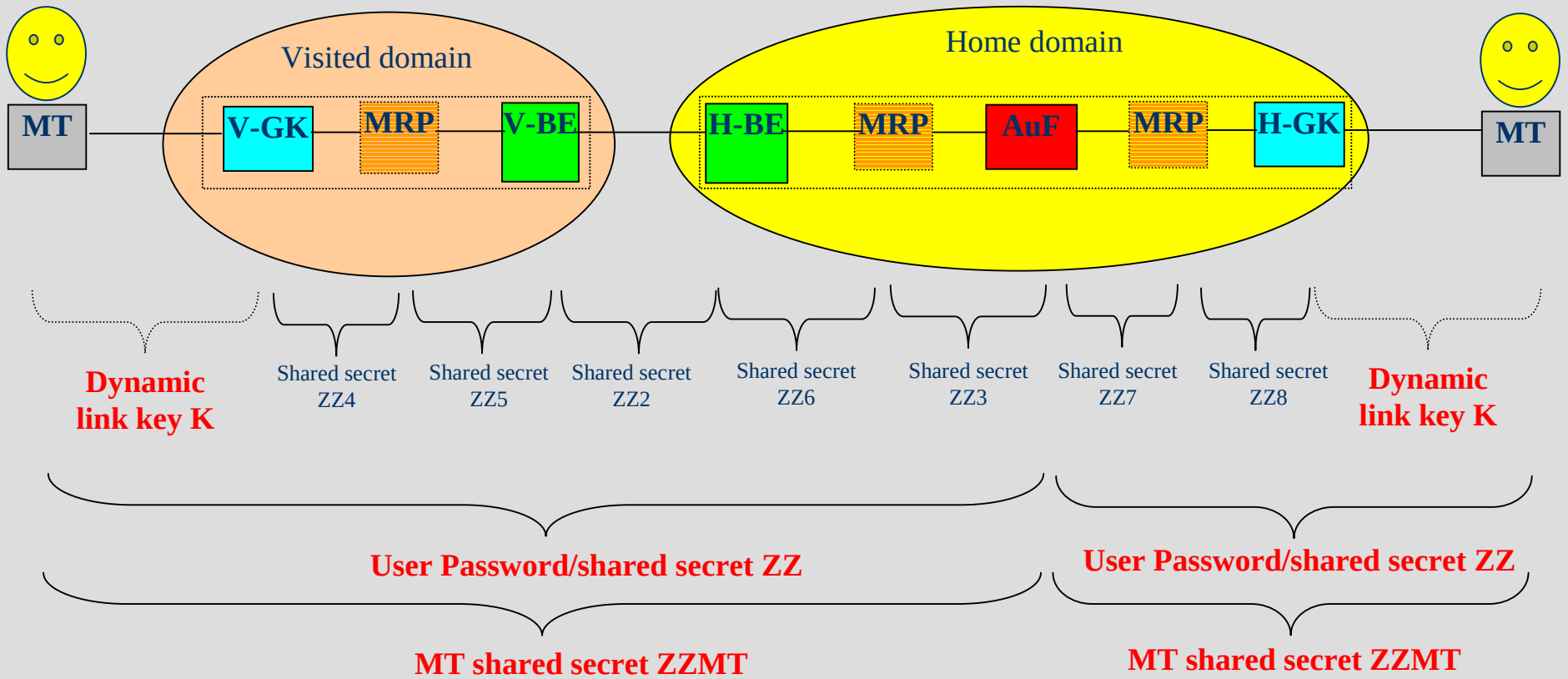
H.248 Security

Secure A/V & Data Conferencing

Secure ETS

- Provide secure user and terminal mobility in distributed H.323 environments beyond interdomain interconnection and limited GK-zone mobility
- Security issues:
  - Mobile Terminal/User authentication and authorization in foreign visited domains
  - Authentication of visited domain
  - Secure key management
  - Protection of signaling data between MT and visited domain

H.530
Scenario and Security Infrastructure



AuF = Authentication Function

MT = H.323 mobile terminal

MRP = mobility routing proxy (HLF, VLF) optional

BE = H.501 Border Element (home/visited)

GK = H.323 Gatekeeper (home/visited)

H.530
Security Protocol

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

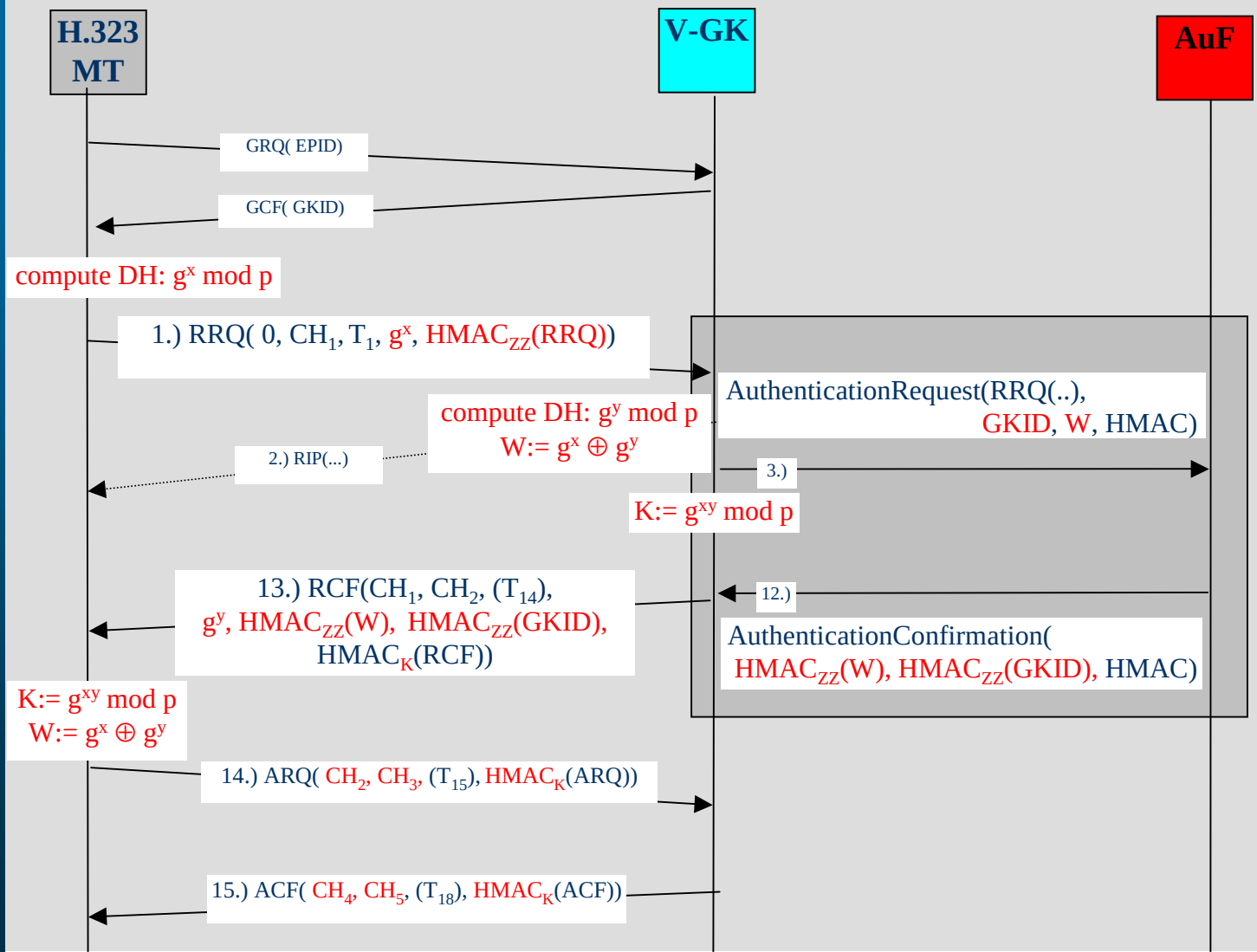
H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS



H.530

"Symmetric Security Procedures for H.510 (Mobility for H.323 Multimedia Systems and Services)"

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

⇐

H.248 Security

Secure A/V & Data Conferencing

Secure ETS

- Works entirely with a shared-secret Security Infrastructure
  - deploys H.235 Annex D (Baseline Security Profile)
  - re-uses H.235 Clear- and CryptoTokens
  - Implementable with H.235 Version 2
  - H.235 and/or IPSEC on hop-by-hop H.501 links between visited domain and home domain and among entities
- Visited domain relays the task of MT/user authentication and authorization to the home domain (AuF)
  - MT authentication/authorization procedure may be executed either at GRQ or RRQ
  - MT authentication may be accomplished piggy-backed in conjunction with user authentication.
  - Having obtained authorization credentials, the visited domain operates "locally" without further interaction with the home domain.
- Does not assume synchronized time between MT and visited domain.
- Works also for the MT in the home domain respectively.
- MRP are optional security proxies (HLF, VLF).

H.530 Procedure

- V-GK encapsulates received MT registration message, forwards to AuF
- AuF verifies MT registration message (MT authentication)
- AuF creates certified credentials for the MT and performs authorization check
- V-GK receives AuF authorization result, may additionally enforce its own authorization policy
- V-GK and MT establish a dynamic Diffie-Hellman session key
- MT verifies obtained certified credentials
- MT and V-GK apply the established key for message protection using a mutual challenge-response protocol (based on H.235 Annex D)

H.530 Security Properties

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

⇐

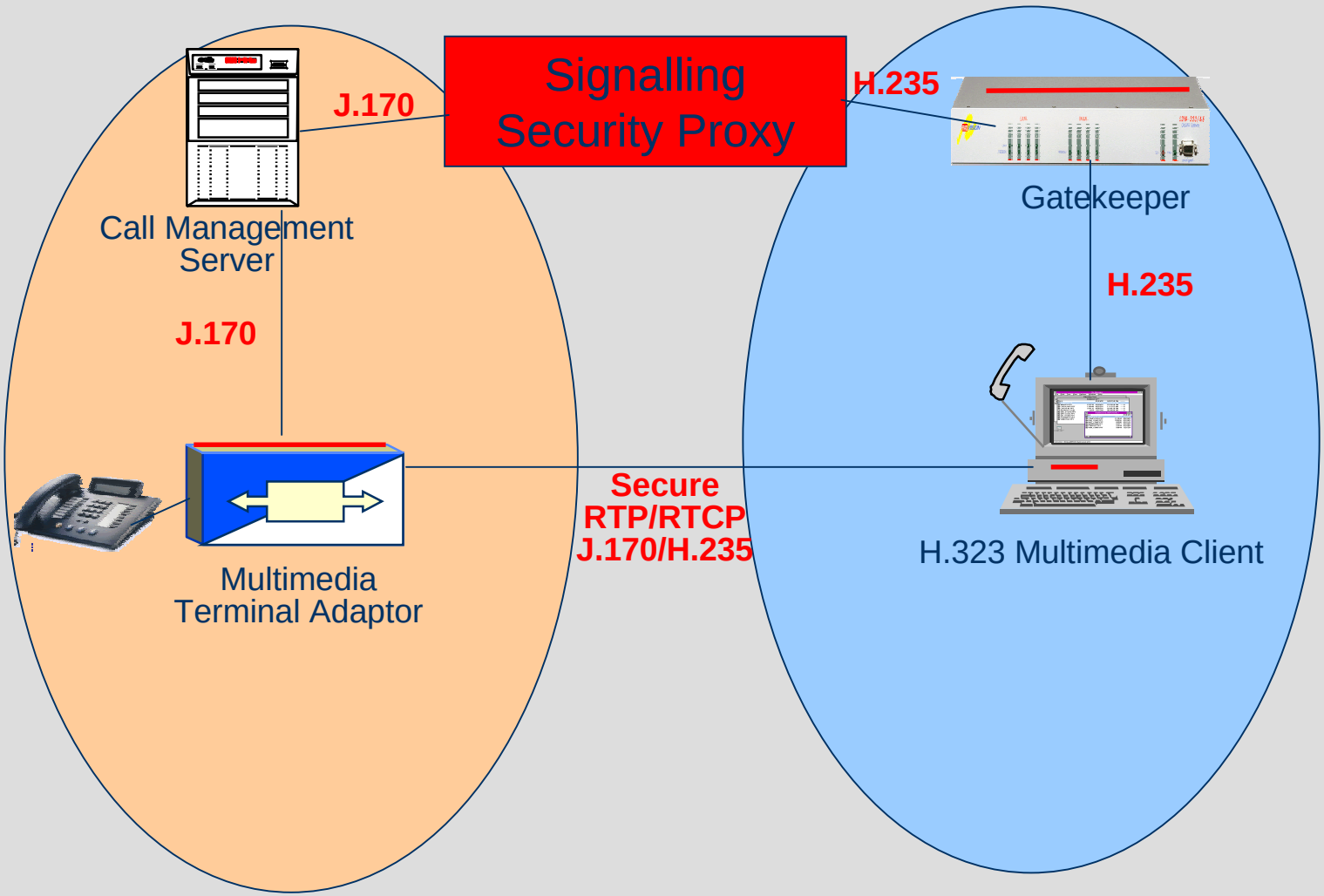
H.248 Security

Secure A/V & Data Conferencing

Secure ETS

- Dynamic session key only available to MT and V-GK, but not to anyone else!
- No encryption usage in the back-end, integrity is fully sufficient there.
- V-GK can not cheat by replay, shortcut attacks (enforced by W)
- Explicit authentication of the MT/user by the AuF
- Implicit authentication between V-GK and AuF relying on mutual trust relationship(s)
- Mutual authentication among MT and V-GK
- Fair session key agreement with Diffie-Hellman
- Guaranteed fresh session key (enforced by W)
- Agreed session key is tested for correctness
- Formal security protocol analysis underway…

Potential H.235 - J.170 Security Inter-working

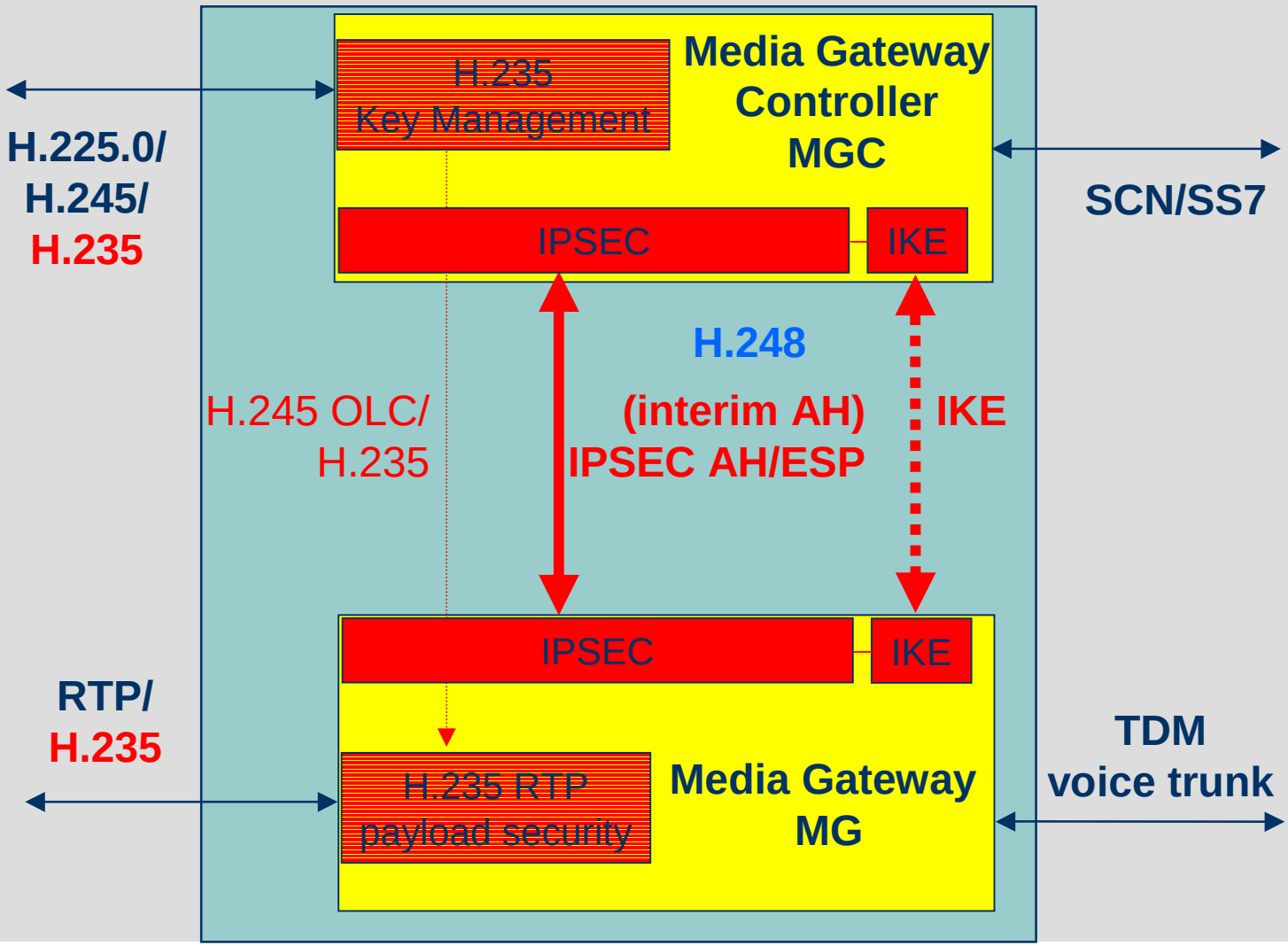


Part III

Media Gateway Decomposition

H.248 Security

H.248 Security in decomposed Gateways



H.248/MEGACOP Security

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security ⇐

Secure A/V & Data Conferencing

Secure ETS

- H.248 applies IPSEC for protection of MGC-MG signaling
  - AH for authentication/integrity of H.248 IP packets
  - ESP for confidentiality/authentication/integrity of H.248 IP packets
- manual keying with administered shared keys mandatory
- IKE for the key management for H.248 session keys recommended
  (default: RSA)
- an optional interim scheme is defined at application layer with AH in front of the H.248 payload for migration until IPSEC is available.

H.248 Message Security

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

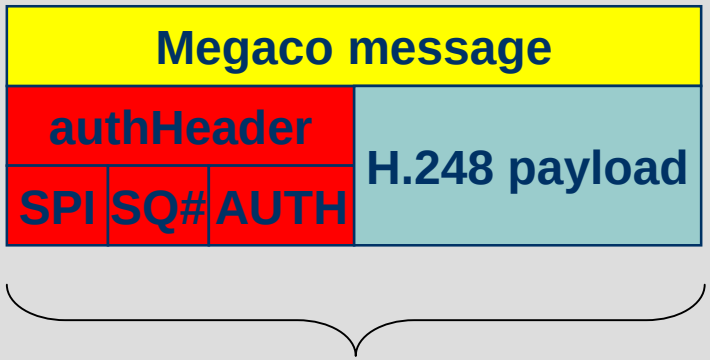
H.530

H.248 Security ⇐

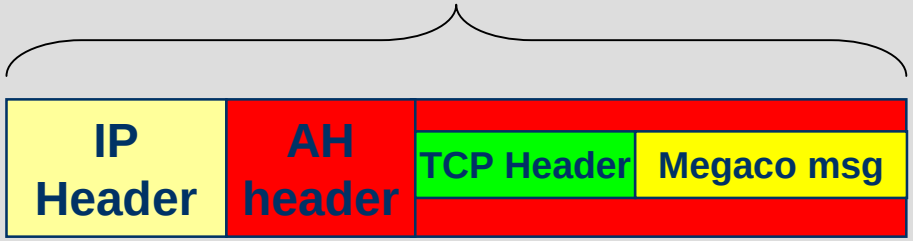
Secure A/V & Data Conferencing

Secure ETS

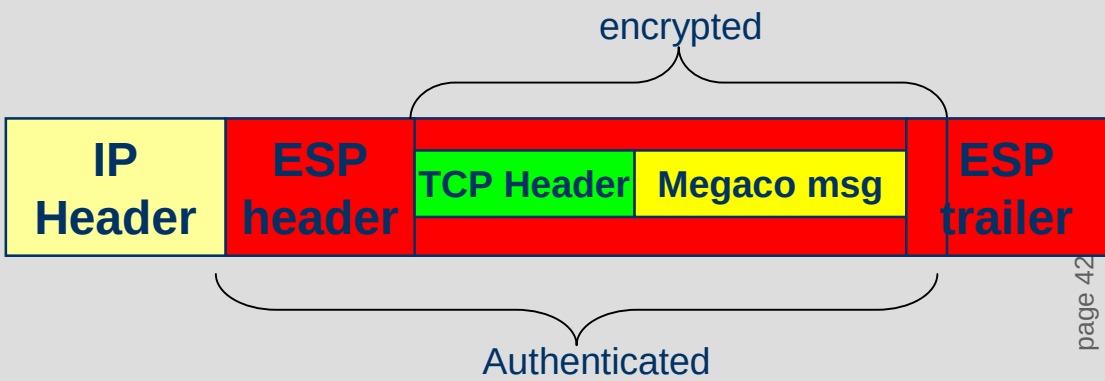
Interim AH scheme:



IPSEC AH:



IPSEC ESP:



Part IV

H.320 Audio/Video Security

Security for Multimedia Terminals on circuit-switched networks

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferenc

Secure ETS

- H.233: “Confidentiality System for Audiovisual Services”
  - point-to-point encryption of H.320 A/V payload data by ISO 9979 registered algorithms: FEAL, DES, IDEA, B-CRYPT or BARAS stream ciphers
- H.234: “Key Management and Authentication System for Audiovisual Services”
  - uses ISO 8732 manual key management
  - uses extended Diffie-Hellman key distribution protocol
  - RSA based user authentication with X.509-like certificates by 3-way X.509 protocol variant

Part V

Security Aspects of Data Conferencing

Security for Computer Supported Collaborative Work (CSCW)

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferenc

Secure ETS

CSCW scenarios:

- Users work in a **virtual office** (Teleworking/Telecommuting from home)
- **collaboration** of users in a tele-conference through a conference system

Security aspects:

- user authentication for granting access to the corporate environment
- telecommuting server can protect out-bound/VPN application data
- secure remote access and management to home office PC
- home office PCs deserve special security protection:
  - against intruders, viruses
  - against misuse of corporate services
  - unauthorized access to local information though application sharing
- point-to-point security may not be optimal in a decentralized multi-party conference

Security for Multimedia Conferencing
T.120 and Security

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

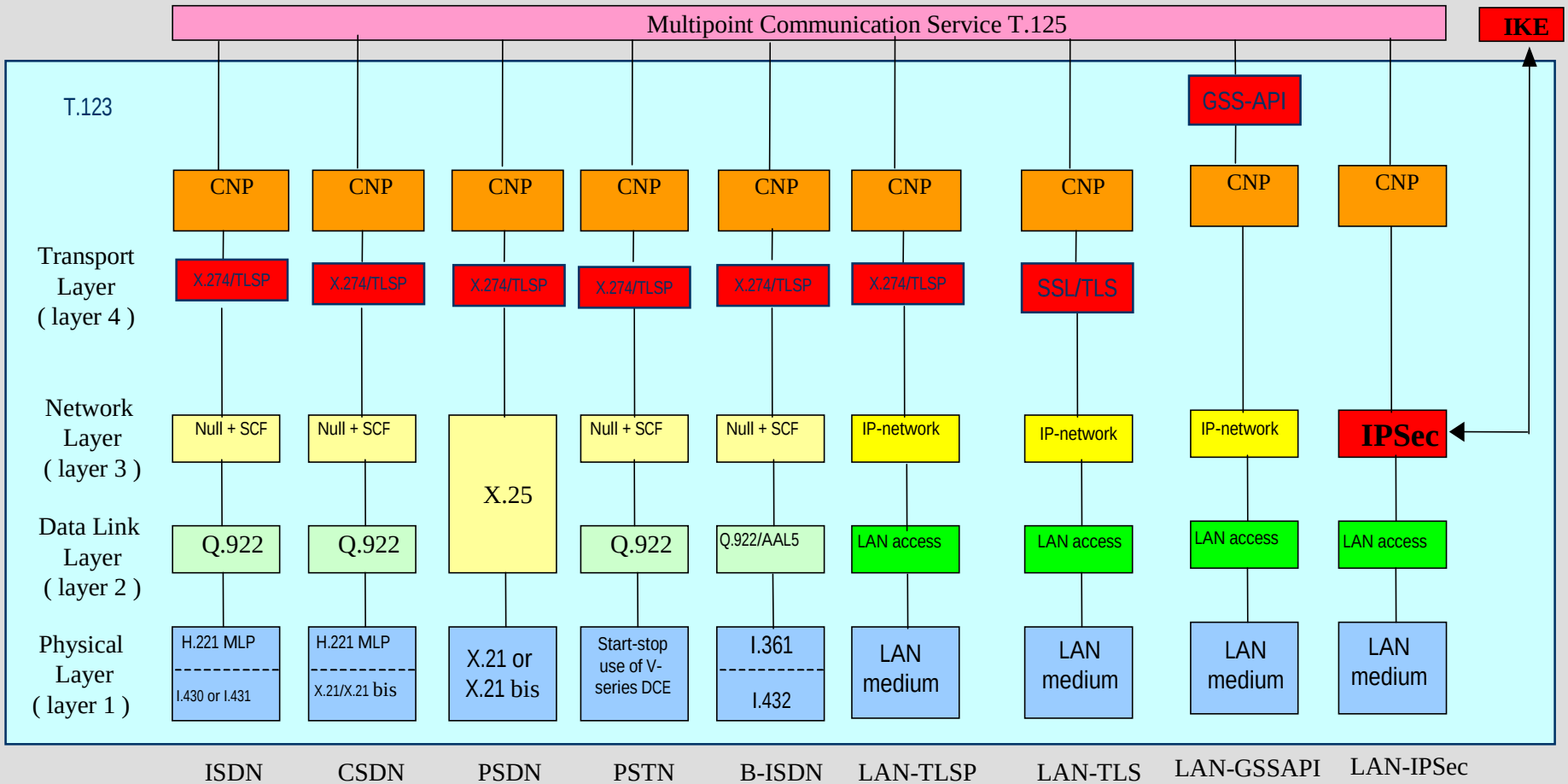
H.248 Security

Secure A/V & Data Conferenc

Secure ETS

- T.120 has very weak information security available (unprotected passwords), common state of the art cryptographic mechanisms are not supported.
- OS security features do not prevent against typical T.120 threats (especially T.128 application sharing vulnerabilities);
  this problem already arises in simple pt-2-pt scenarios.
- Additional threats exist for group-based multipoint scenarios:
  insider threats, lack of access control, “write token” not protected, unsecured conference management ,…
  - The T.120 “**virtual conference room**” needs integral and user friendly security protection: for authentication & role-based authorization, for confidentiality, for integrity, and security policy negotiation capabilities.

T.123 profiles with network security features



T.123 network profiles with security

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferenc

Secure ETS

- Supports network security on a node-to-node basis
  - TLS/SSL
  - IPSEC w/o IKE or manual key management
  - X.274/ ISO TLSP
  - GSS-API
- connection negotiation protocol (CNP) offers security capability negotiation
- secures conference against “out-siders” but does not provide security within a conferences (no access control on applications and GCC conferencing services)
- no support for multipoint/multicast and T.125 MAP
- still relies on “trusted intermediate nodes” but does not offer true end-to-end security across heterogeneous networks

Emergency Telecommunications services
Security for Multimedia Applications and Systems

SG16 & Q.G

Secure IP Telephony

H.235

Annex D

Annex E

Annex F

H.235 V3

H.530

H.248 Security

Secure A/V & Data Conferencing

Secure ETS

- Security objectives:
  - prevent theft of service and denial of service by unauthorized user
  - support access control and authorization of ETS users
  - ensure the confidentiality and integrity of calls
  - provide rapid and user-friendly authentication of ETS users

- H.SETS is the provisional title for a new work item under study within Q.G with the focus on the multimedia security aspects of ETS
- Relationship identified with QoS, network issues, robustness and reliability,...