CableLabs®

IPCablecom Security

Eric Rosenfeld, CableLabs
Sasha Medvinsky, Motorola
Simon Kang, Motorola

ITU IPCablecom Mediacom Workshop
March 13, 2002
Geneva, Switzerland

CableLabs®

Agenda

- IPCablecom Overview
- How it Works
- Services and Capabilities
- Security Goals of IPCablecom
- IPCablecom Security Architecture
- Security Mechanisms & Component
- Summary

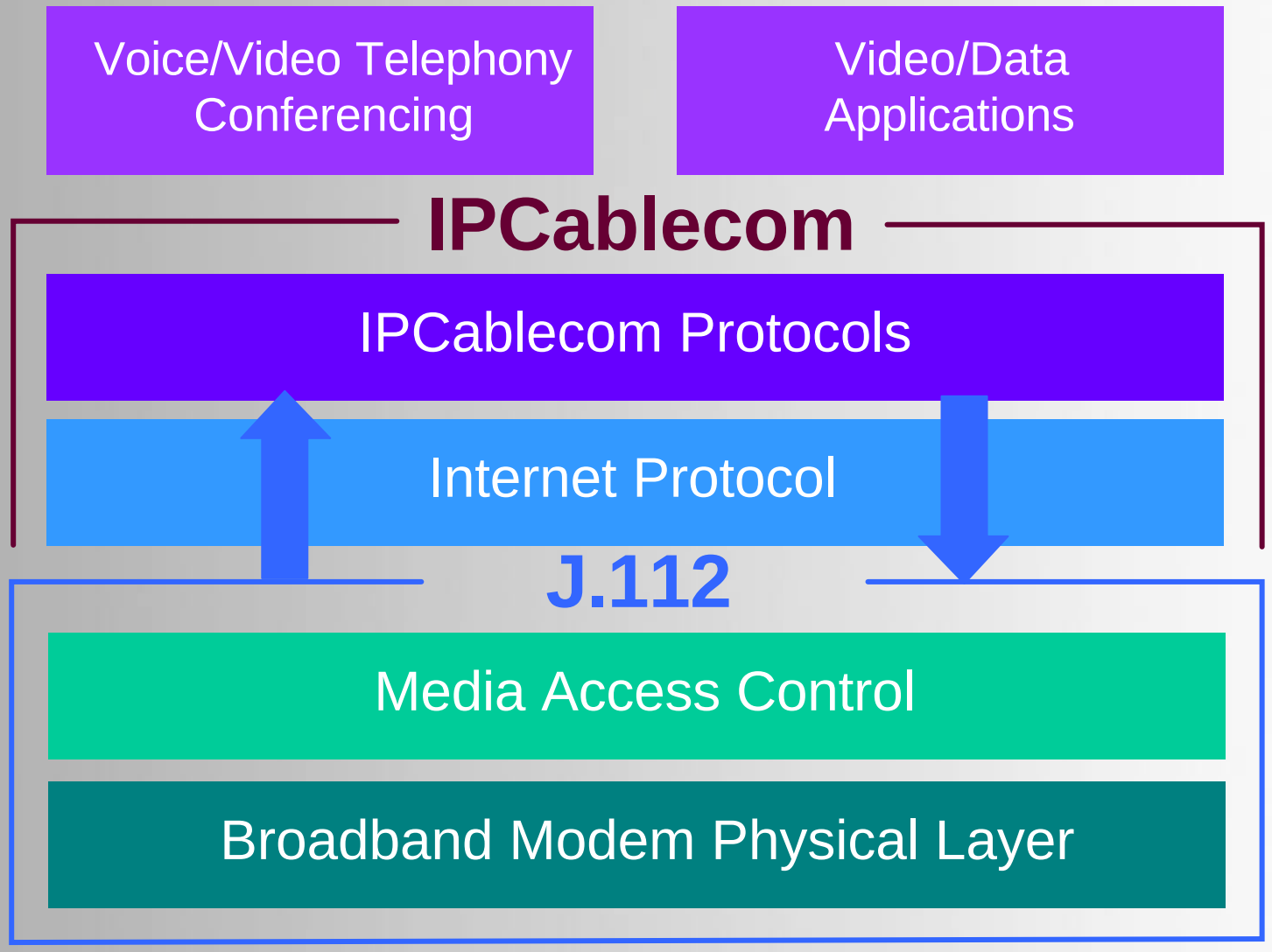
CableLabs®

What is IPCablecom?

IPCablecom is a set of standards that define protocols and functional requirements for the purpose of providing Quality-of-Service (QoS) enhanced secure communications using the Internet Protocol (IP) over the cable television Hybrid Fiber Coax (HFC) J.112 network

CableLabs®

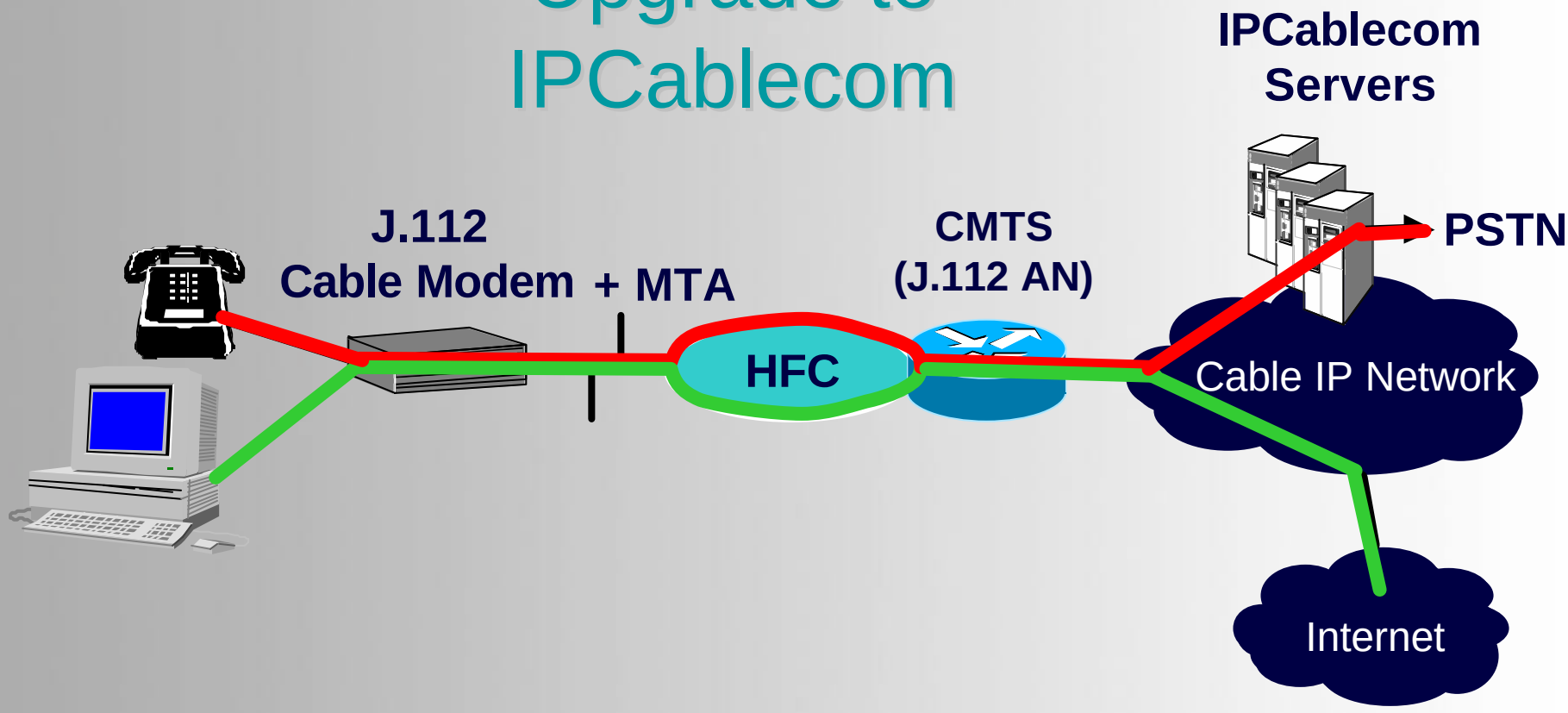
IPCablecom Framework



CableLabs®

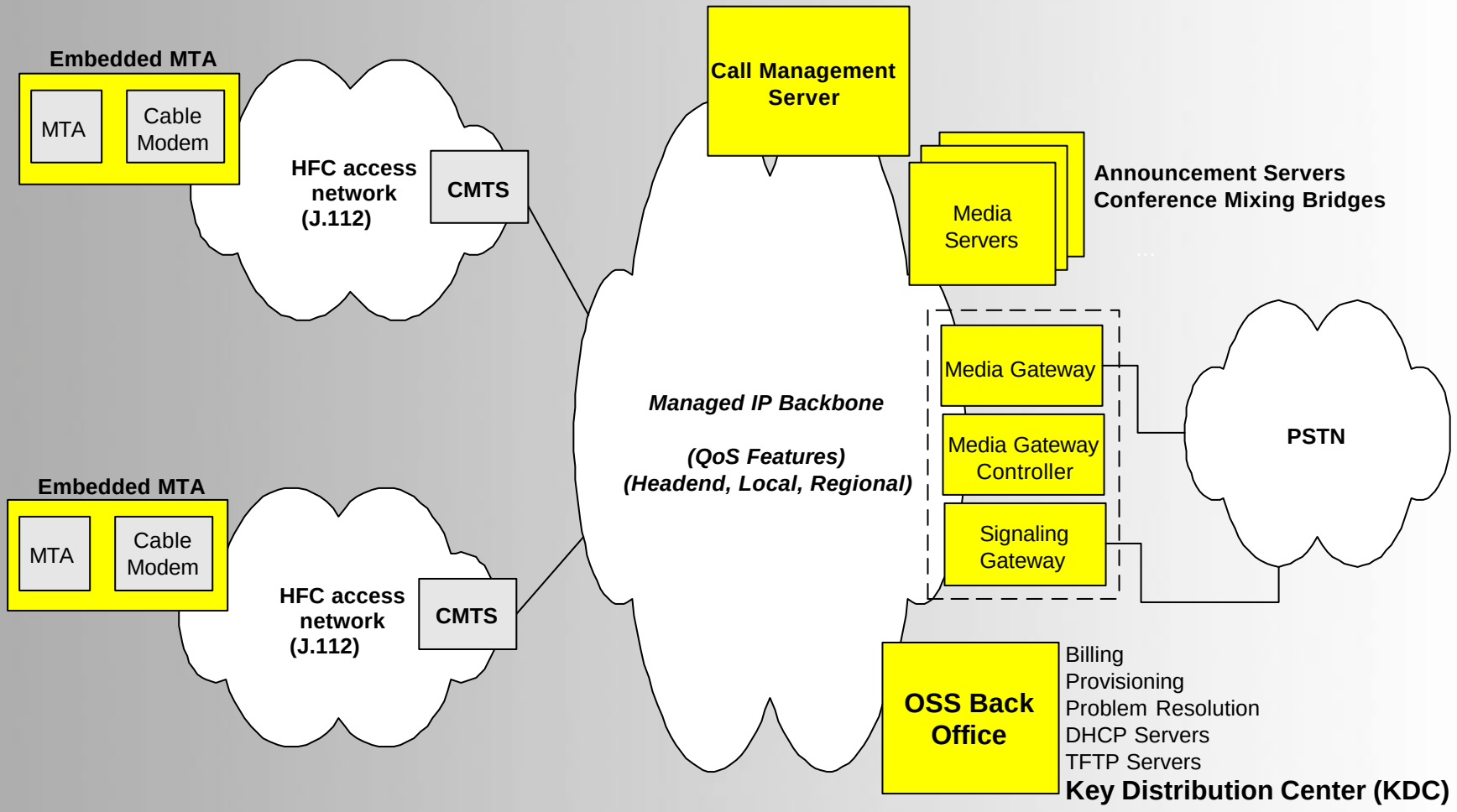
IPCablecom How it Works

Upgrade to IPCablecom



CableLabs®

IPCablecom Architecture



CableLabs®

IPCablecom : What Equipment?

- Home:
  - Embedded Multimedia Terminal Adapter (MTA) -- cable modem with RJ-11 jacks
- Headend:
  - Cable Modem Termination System (CMTS): J.112 AN
  - IPCablecom Servers: Call Management Server (CMS), Record Keeping Server (RKS), Device Provisioning Server, Key Distribution Center (KDC)
  - Gateways: To link IP calls to backbone or PSTN

CableLabs®

And now the security…

CableLabs®

Why do we need security?

- Threats to the IPCablecom Network
  - Threats exist because:
    - Shared network
    - Access in the users home
    - Valued functionality
  - Types of threats:
    - Network attacks
    - Theft of service
    - Eavesdropping
    - Denial of Service

CableLabs®

Security Services provided by J.112

- Baseline Privacy Interface + (BPI+)
  - Privacy between the Cable Modem and CMTS
    - DES encryption
  - Protection from theft of Service
    - Authentication of Cable Modems via X.509 digital certificates
  - Enable secure code download to the Cable Modem
    - Authentication of Cable Modem software image via X.509 Code Verification Certificate

CableLabs®

BPI+ Applicability to IPCablecom

- Embedded MTAs rely on Cable Modem for secure code download
- Privacy of J.112 QoS messages prevents some denial of service attacks
- Theft of Service protection doesn't apply:
  - CPEs behind a CM are not authenticated
  - IP Telephony servers also not authenticated
- Additional security at application layer is needed to protect IPCablecom services

CableLabs®

IPCablecom Security Objectives

- End-to-end secure communication
  - Must be at least as secure as PSTN networks
- Protection for the user
  - Ensure privacy of media sessions
- Protection for the operator
  - Combat theft-of-service
  - Protect infrastructure
- Comprehensive plan
  - Who/What needs to protect and why?
  - When/Why do we protect this information?
  - How will we incorporate security?

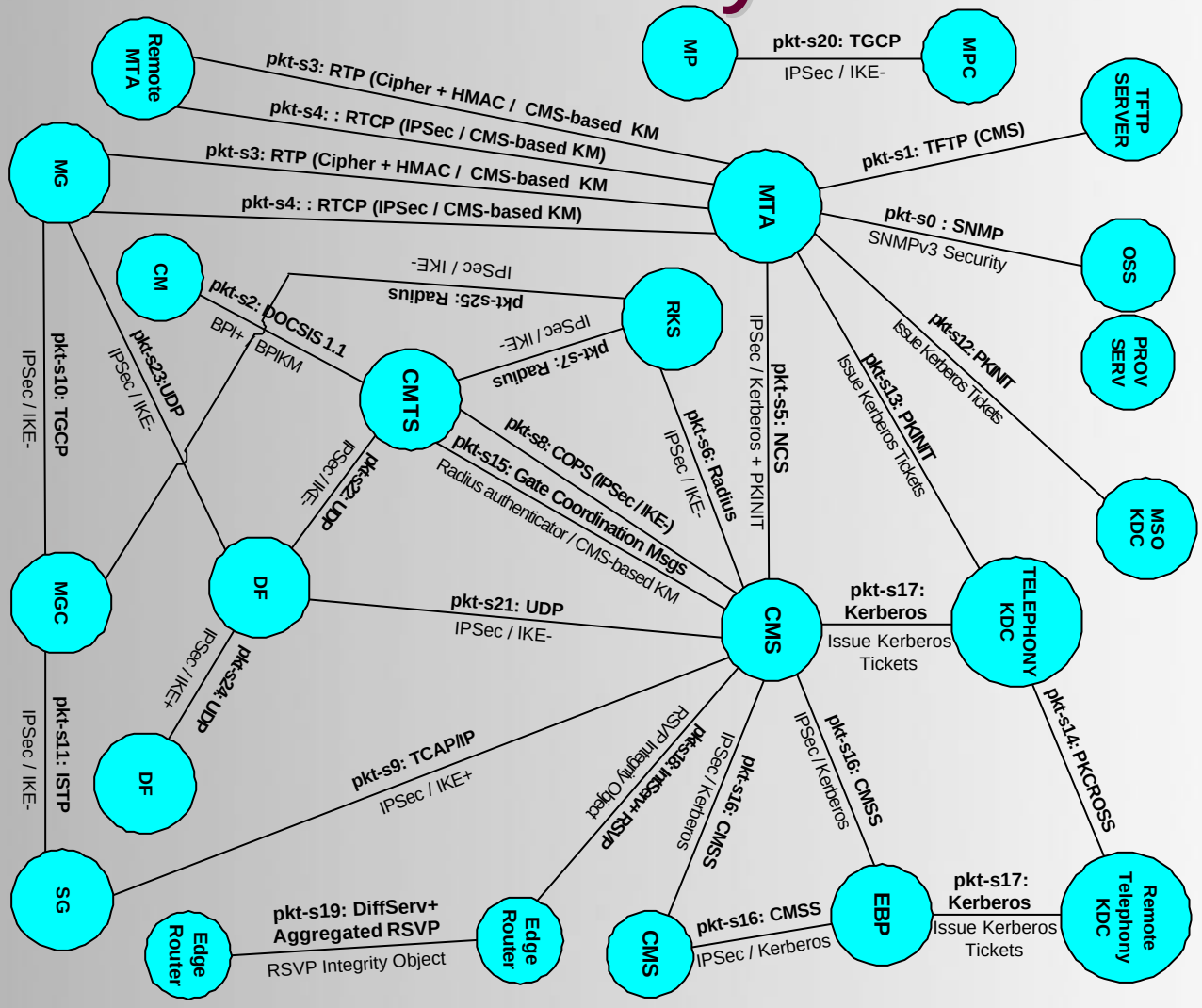
CableLabs®

IPCablecom Security Objectives

- Use open standards whenever possible
- Conduct a risk assessment
- Provide a reasonable level of security
- Specify Interface security
  - No device or operator network security
    - Assume operators must have reasonable network management security policy
- Require J.112 networks with BPI+ enabled

CableLabs®

IPCablecom Security Architecture



CableLabs®

Security Mechanisms

- Kerberos
  - Centralized network authentication via a Key Distribution Center (KDC)
  - Public Key Initialization (PKINIT)
    - Digital Certificates are used to authenticate the MTA to the KDC and KDC to MTA
  - Key Management
    - Allows MTAs and CMSs to agree on cryptographic keys for secure communications

CableLabs®

Security Mechanisms

- IPsec
  - IP-layer security protocol (IETF standard)
  - Encapsulating Security Payload (ESP)
    - Transport mode for end-to-end security
    - Privacy/authentication/integrity of payload
      - 3DES, HMAC SHA1 or HMAC MD5
  - Initial Authentication & Key Management provided by:
    - Kerberos+PKINIT for MTAs
    - Internet Key Exchange (IKE) with pre-shared keys for infrastructure components (CMS, CMTS, RKS, Gateways)

CableLabs®

Security Mechanisms

- SNMPv3 security
  - SNMPv3 is used to monitor & manage MTAs
  - Initial Authentication & Key Management
    - Kerberos+PKINIT
  - Message Authentication & Integrity
    - HMAC MD5 algorithm
  - Privacy (optional)
    - DES algorithm

CableLabs®

Security Mechanisms

- Call Signaling Security
  - NCS, TCAP/IP, ISTP, and TGCP Protocols
  - Protocol security provided by IPsec
  - Mix of authentication & key management technologies:
    - IKE with pre-shared keys for servers
      - Default for IPsec, comes bundled with off-the-shelf implementations
    - Kerberos+PKINIT for MTAs
      - Needed to address scalability issues on the CMS-MTA interface

CableLabs®

Security Mechanisms

- RTP/RTCP (Media Stream)
  - Initial Authentication
    - Each end-point (MTA or MG) authenticated by the Call Management Server
  - Key Management
    - Via IPsec-secured Network-based Call Signaling (NCS)
  - Privacy
    - Advanced Encryption Standard (AES)
  - Authentication & Integrity (optional)
    - MMH (Multilinear Modular Hash)

CableLabs®

Key Distribution Center (KDC)

- The only standalone security component in IPCablecom
- Acts as a trusted third-party authentication service
- Implements:
  - Kerberos version 5
  - PKINIT w/X.509 digital certificates

CableLabs®

Multimedia Terminal Adapter

- X.509 Digital Certificates for authentication
  - IP Telephony Root CA Certificate
  - MTA Manufacturer CA Certificate
  - MTA Device Certificate
    - MTA Private Key
- FIPS 140-1 Cryptographic Module
  - Level 1 required (minimal physical security)
  - Additional physical security recommended for higher value services
- Random Number Generator
- AES, MMH, IPsec, Kerberos+PKINIT
- Embedded J.112 CM with BPI+

CableLabs®

Device Provisioning Server

- Authentication & Key Management
  - Kerberos+PKINIT authentication
- Integrity & Privacy
  - SNMPv3 security
    - Authentication
      - HMAC MD5
    - Privacy (optional)
      - DES

CableLabs®

PSTN Gateways

- Media Gateway Controller (MGC)
  - IPsec,IKE w/pre-shared keys for call signaling
- Media Gateway (MG)
  - AES, MMH for media stream
  - IPsec, IKE w/pre-shared keys for call signaling
- Signaling Gateway (SG)
  - IPsec, IKE w/pre-shared keys for call signaling

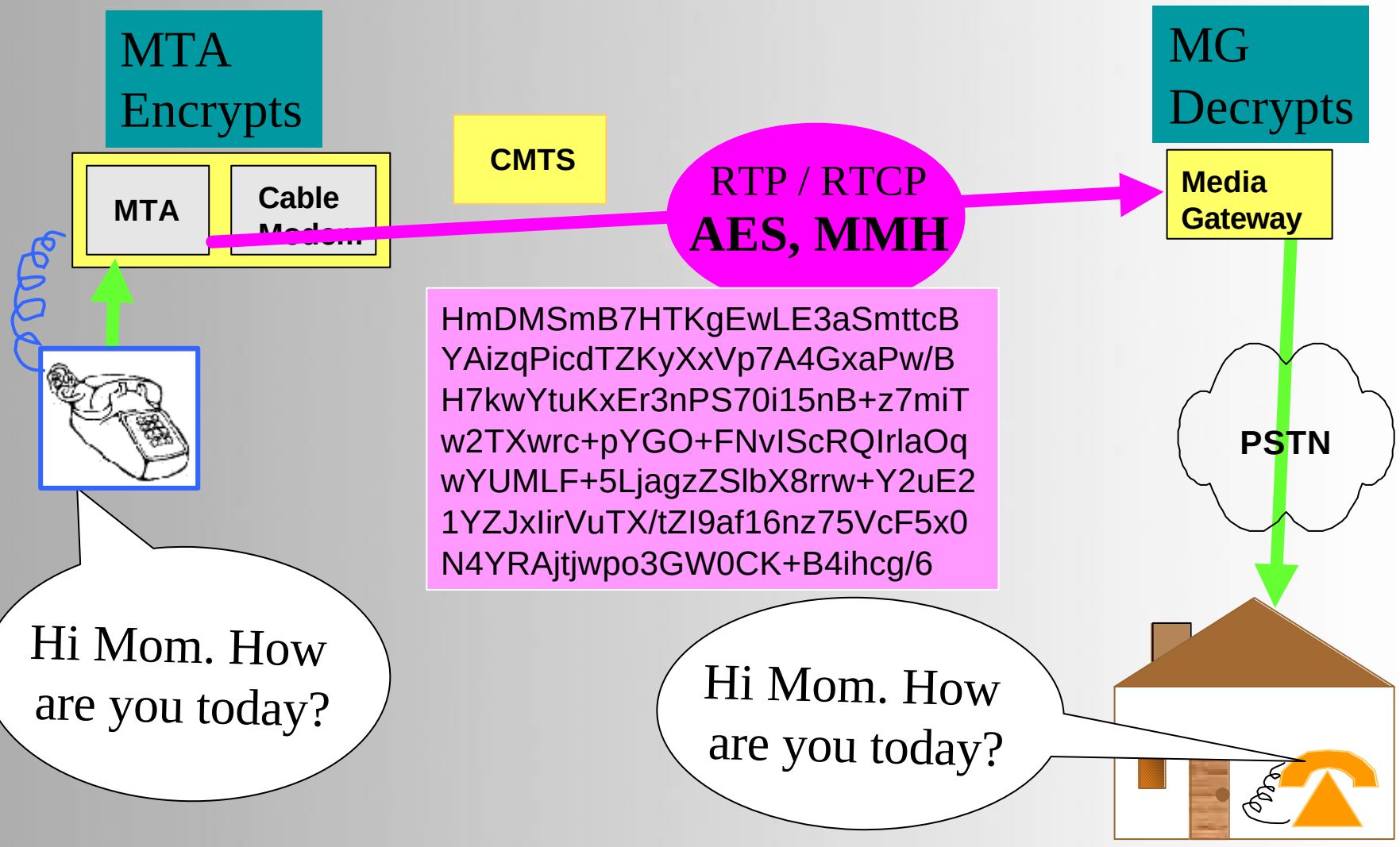
CableLabs®

Other Components

- Cable Modem Termination System (CMTS)
  - J.112 Access Node (AN) w/BPI+
  - IPsec w/pre-shared keys and RADIUS authentication for QoS interface with CMS
- Call Management Server (CMS)
  - IPsec w/pre-shared keys
  - IPsec w/Kerberized Key Management for MTAs
- Record Keeping Server (RKS)
  - IPsec w/pre-shared keys for billing events

CableLabs

On-Net to Off-Net Media Path



CableLabs®

Summary

- IPCablecom provides QoS-enhanced secure communications
- Security is a major component and is integrated into the architecture
- A range of security protocols and services are used
- IPCablecom security architecture is fully defined in the J.170 recommendation

CableLabs®

For More Information…

Eric Rosenfeld
CableLabs
PacketCable Security Architect
e.rosenfeld@cablelabs.com

Sasha Medvinsky
Motorola
Senior Staff Engineer
smedvinsky@motorola.com

Simon Kang
Motorola
International Regulatory and Standards Specialist
simonkang@motorola.com