Securing the Mobile Environment with IP-VPNs

SSH Communications Security, Inc.
David Precopio, Sr. Product Manager

Agenda

? Mobile and WLAN

  ? Definitions

? Handhelds

? Mobile Technologies and Issues

? 3G Wireless Security

? Virtual Private Networks

  ? Wireless IP VPN

  ? Secure Shell

  ? Future

Issues with Mobile Internet

? From WAP or i-mode to “all IP” 3G

- Band-aid security

? Fixed / mobile convergence

? Mobile versus other wireless

? Cell Phones vs PDAs vs Laptops, etc

? Who validates user access and transaction?

Wireless Environments

- ? How to define “true” mobile and wireless Internet
- ? Mobile
- ? WLAN
  - ? 802.11x
  - ? Bluetooth
- ? Fixed Broadband
  - ? 802.16
  - ? MMDS
  - ? OFDM, VOFDM

Technologies of Mobile Internet

? 2G standards

? 2.5 G standards
GPRS, EDGE, CDMA-P, PDC-P

? 3G standards
w-cdma, cdma2000, cdmaHDR

? Applications Protocols
WAP and i-mode

? Future non mobile wireless
BlueTooth, WLAN IEEE 802.11

? Fixed/mobile convergence
Internet Protocol (IP) as common network denominator
Public Key Infrastructure (PKI) as common certification

What is a Wireless LAN

- ? Basically it is Ethernet with a medium range wireless functionality
- ? Operates in the unlicensed RF spectrum (add range)
- ? Commonly known as IEEE 802.11
- ? Currently offering 11Mbps (802.11b) - 22 Mbps coming soon
- ? Standards emphasize wireless networking

WLAN Market

? Wireless LANs driven by:

  ? **Recent adoption of IEEE 802.11(b) standard**

  ? **11 Mbps speeds actually being achieved**

  ? **Lower costs**

  ? **Anytime, anywhere “mobile” computing**

? 2.4 GHz band is:

  ? **Available without a license**

  ? **Available Globally**

Wireless Handhelds

- ? PDA
  - ? Palm Pilots
  - ? Pocket PC
  - ? Compaq iPAQ
  - ? RIM Pagers
- ? PDA & telephone
  - ? Nokia Communicator (9290 US)
  - ? Samsung SPH-1300

Palm VIIx

Nokia 9210 Communicator

Handheld Devices

? New wireless communication technologies provide more bandwidth

  ? Reduces need for single-purpose proprietary communications protocols

? Increased processing power of terminals enables complex cryptographic operations

? Memory capacities also increasing, allowing implementation of more generic but complicated protocols.

? All of the above enable the use of

  ? IPv4 & IPv6

  ? IPSec

2G

? The built-in security mechanisms of 2G wireless technologies are insufficient by current standards

? More reliable security features can be built to transport or application levels

  ? Implementation of PKI on SIM cards

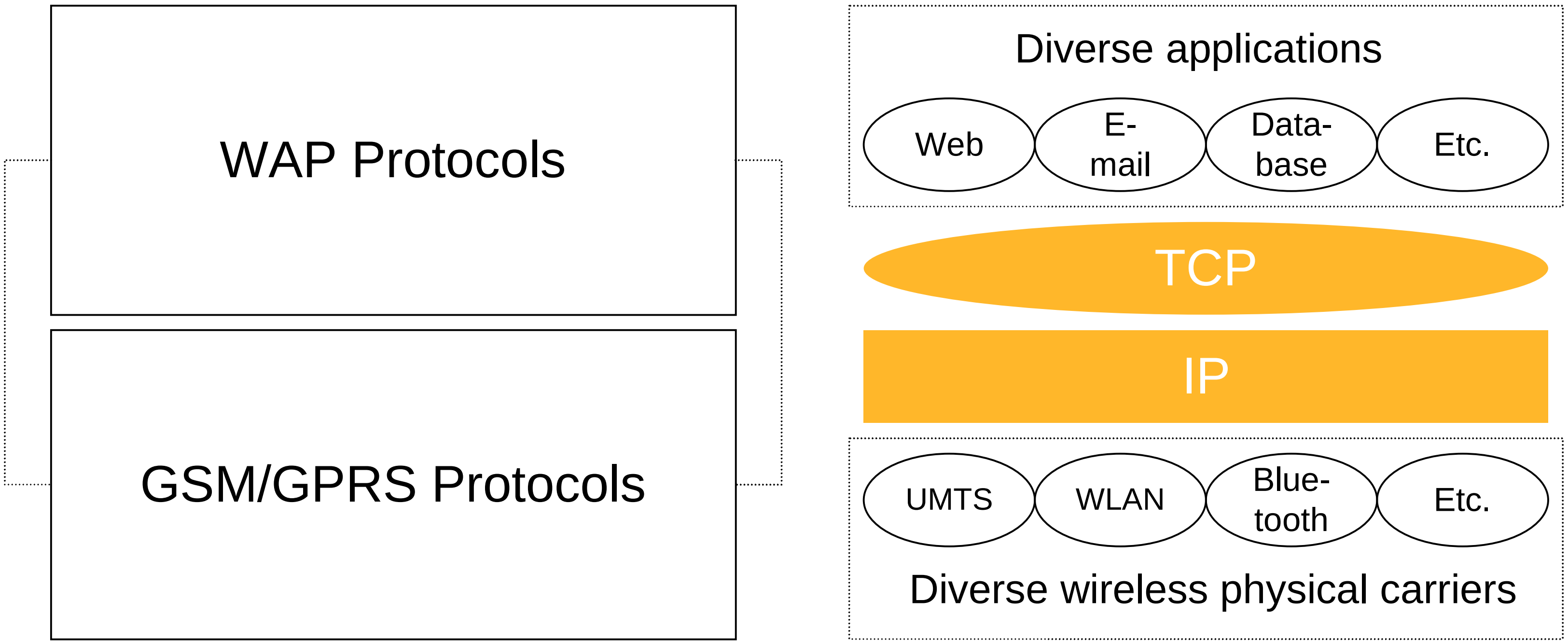
  ? Security mechanisms of WAP

? WTLS does not provide end-to-end security

3G Security and Beyond

- ? Wireless broadband access allows sufficient capacity for TCP/IP
- ? Security mechanisms of wired Internet should be used to guarantee interoperability
- ? Large number of terminals mandates use of IPv6
- ? Convergence to the standards of Internet Engineering Task Force (IETF)

Different Approaches to the Wireless Internet



GSM/GPRS + WAP

WAP Protocols

GSM/GPRS Protocols

TCP/IP-based wireless Internet

Diverse applications

Web

E-mail

Database

Etc.

TCP

IP

UMTS

WLAN

Bluetooth

Etc.

Diverse wireless physical carriers

IP Layer Security

? IPSec forms the backbone of all IP-based security

? IPSec is a mandatory part of IPv6 specifications

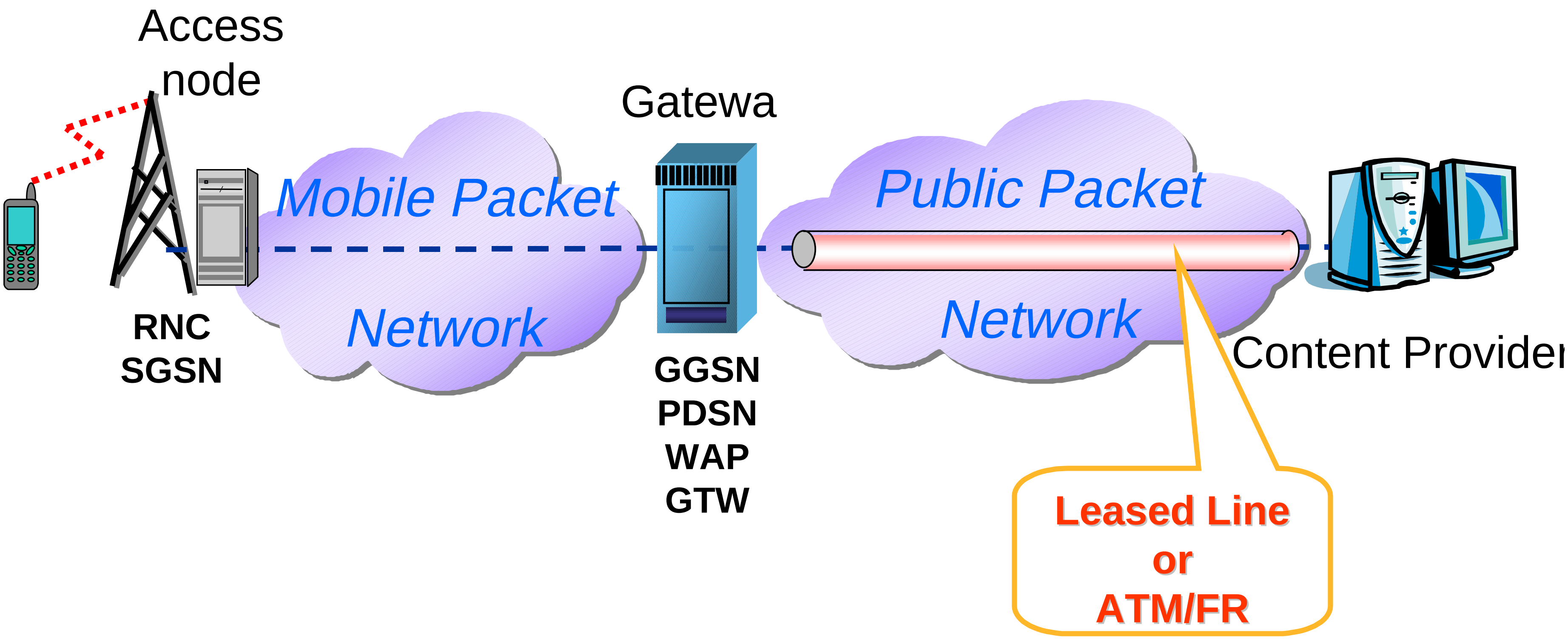
? Establishment of an end-to-end Security Associations

? Authentication by shared keys (IKE) or PKI Digitals Certificates

? IPSec and PKI together form a scalable end-to-end security solution for all applications and networks

2.5 G/3G Network

Mobile Packet Network



Access node

RNC
SGSN

Mobile Packet

Network

Gatewa

GGSN
PDSN
WAP
GTW

Public Packet

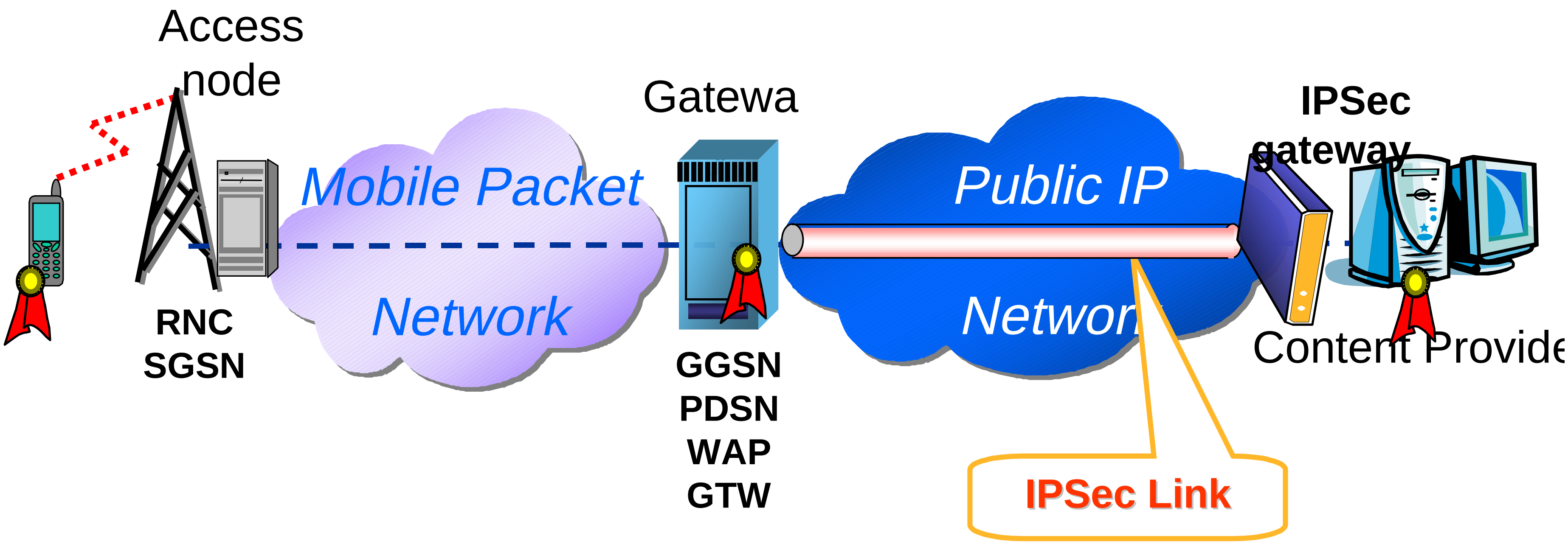
Network

Content Provider

Leased Line
or
ATM/FR

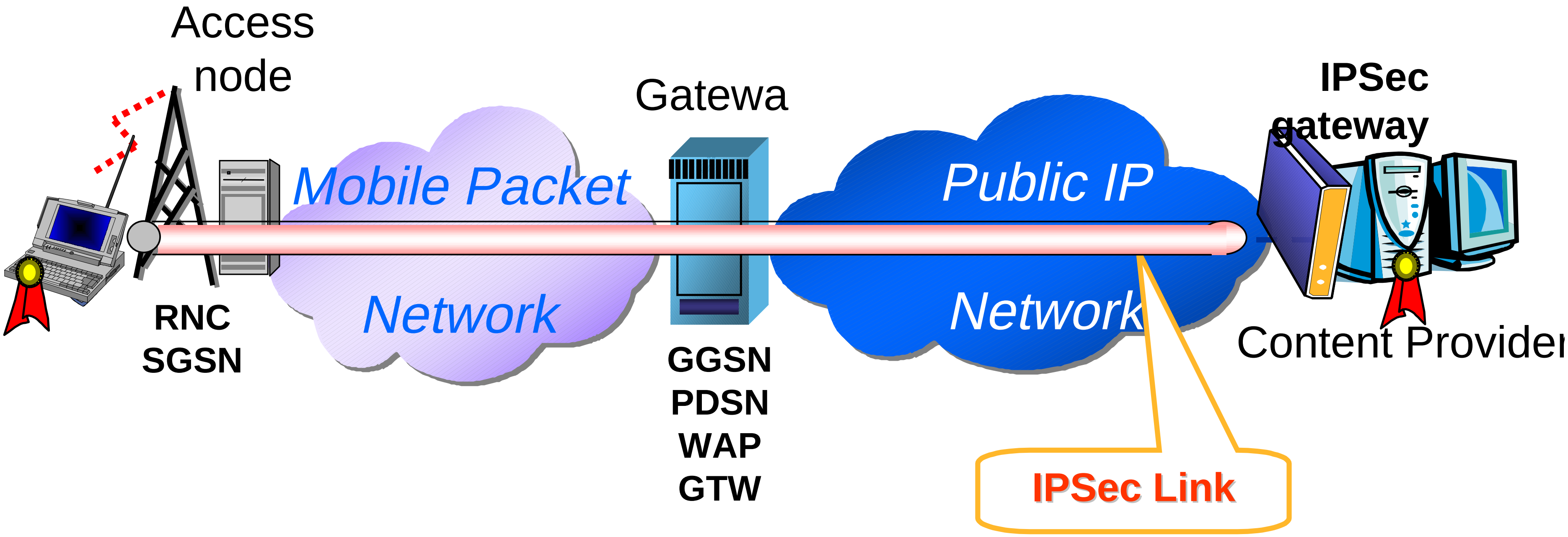
2.5G/3G Network

Implementing IPSec



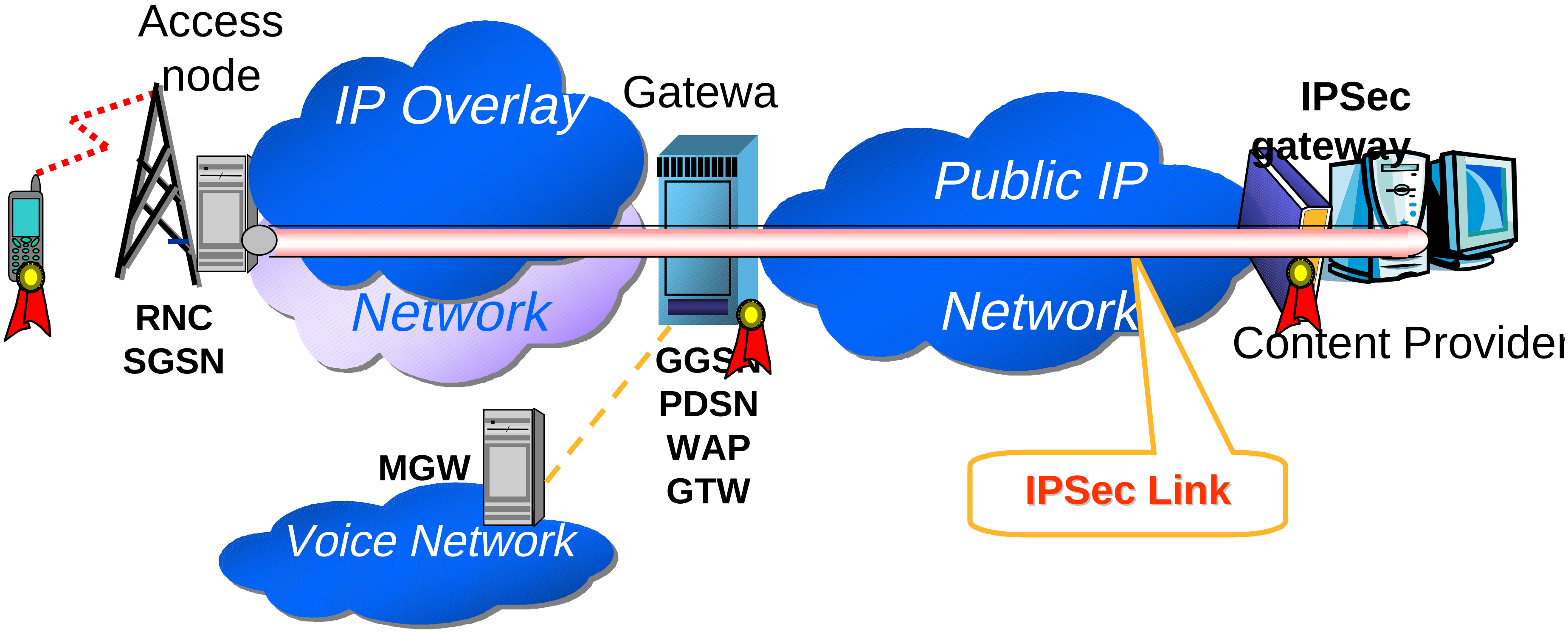
2.5G/3G Network

Implementing end-to-end IPSec connection



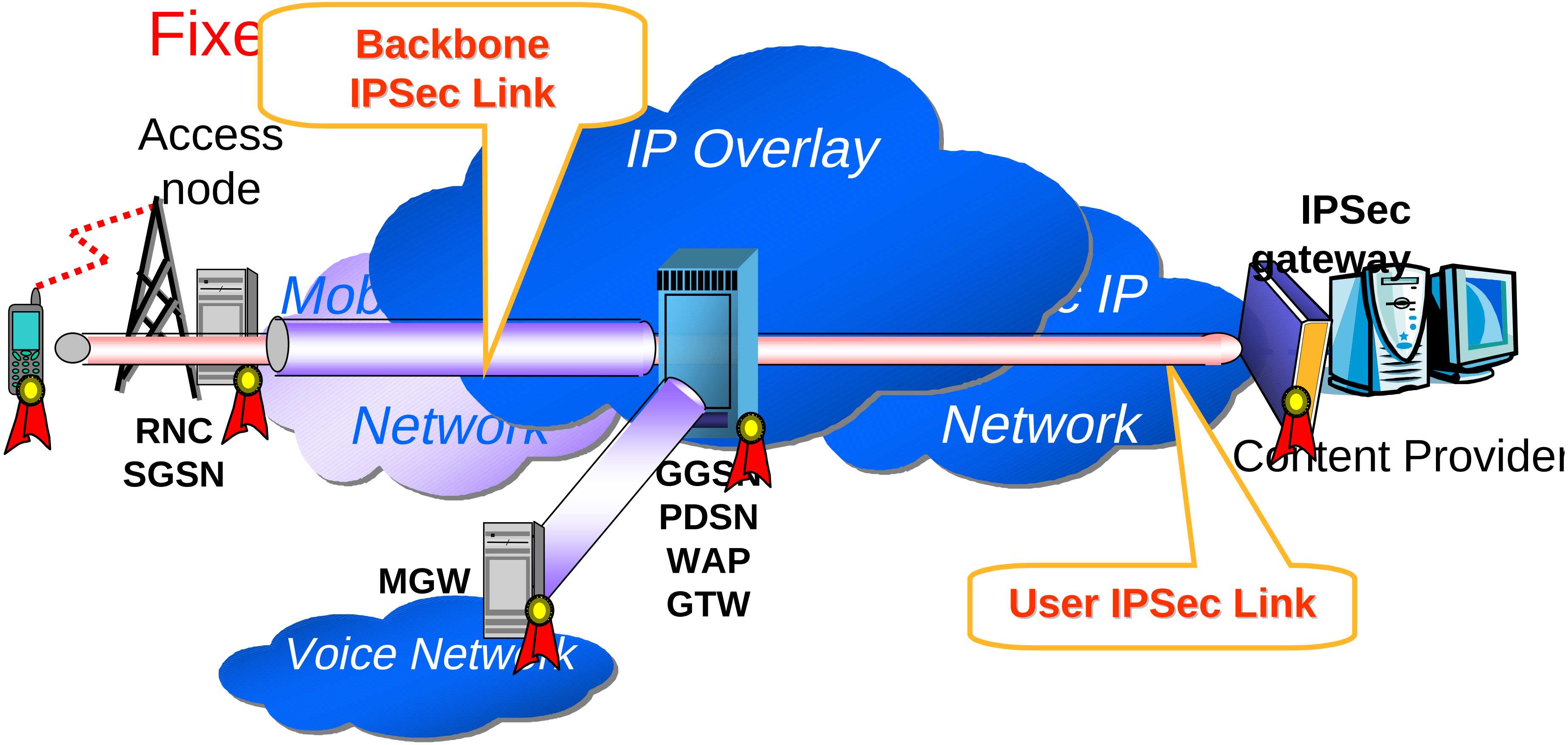
Preliminary 3G IP

IPSec



Final all IP 3G

Implementing IPSec through unified Mobile / Fixe



Conclusion

? Current 2.5G / 3G focused

- WTLS + WPKI is possible now?
- IPSec + WPKI with VPN Client

? Progressive penetration of IP in later 3G

- IPSec to enter the backbone

? Future all IP end-to-end

- Multi-tunneled IPSec end-to-end

Virtual Private Networks

“Secure access to corporate resources by field offices, remote users and business partners”

? **Business Level Process**

? **Encryption and Authentication**

Ultimate Goal:
IP access with PKI to
any user Wired
and Wireless

VPN Technologies

? **IPSec**: Authentication & Encryption Components

  ? Specified in IPv6, widely ported in IPv4

? **PPTP**: Point-to-Point Tunneling Protocol

? **L2TP**: Layer 2 Tunneling Protocol (L2F +PPTP)

? **SOCKS**: NEC Firewall Transversal Tunneling Protocol

? **NAT-T**: NAT Traversal

? **SSH**: Secure Shell

VPN Comparison

Feature	L2F	PPTP	L2TP	IPSec	SOCKS	SSH
Multi-protocol	Yes	Yes	Yes	No	No	No
End host authentication	Yes	NO	Yes	Yes	Yes	Yes
User authentication	No	Yes	Yes	Prop	Yes	Yes
Tunneling	Yes	Yes	Yes	Yes	Proxy	Yes
Data encryption	No	Yes	IPSec Prop	Yes	Yes	Yes

Wireless IP VPN

? Use of current VPN solutions for WLAN

  ? Wireless Secure Gateways

  ? IPSec Clients - Client to Firewall configuration

  ? WEP – better than nothing?

  ? PDA using IP/ WLAN technology

? Currently, no “true” IP Mobile VPN solution

? Mobile security at the application layer

? PKI with WPKI

Mobile Secure Shell

? Secure Shell

  ? Security at the application layer

? Flavors of Secure Shell from many providers and open source

  ? Secure Shell for Handhelds provides a “Current” opportunity for “Lite” VPN for the mobile market

  ? Secure end-to-end communications

  ? Used over many platforms

Conclusion

- ? Technology needs to reach Mobile IP- VPN
- ? Continue the IPSec – Standard
- ? NAT-T development and standardization
  - ? NAT devises must be tested and working
- ? Mobile and PDA market move towards IP
  - ? 3G
- ? Increase in devises will enhance need IPv6