iDEN and Public Safety Communications

The International Emergency Management Society

International Workshop 2004

February 12-13, 2004

MOTOROLA

intelligence everywhere™

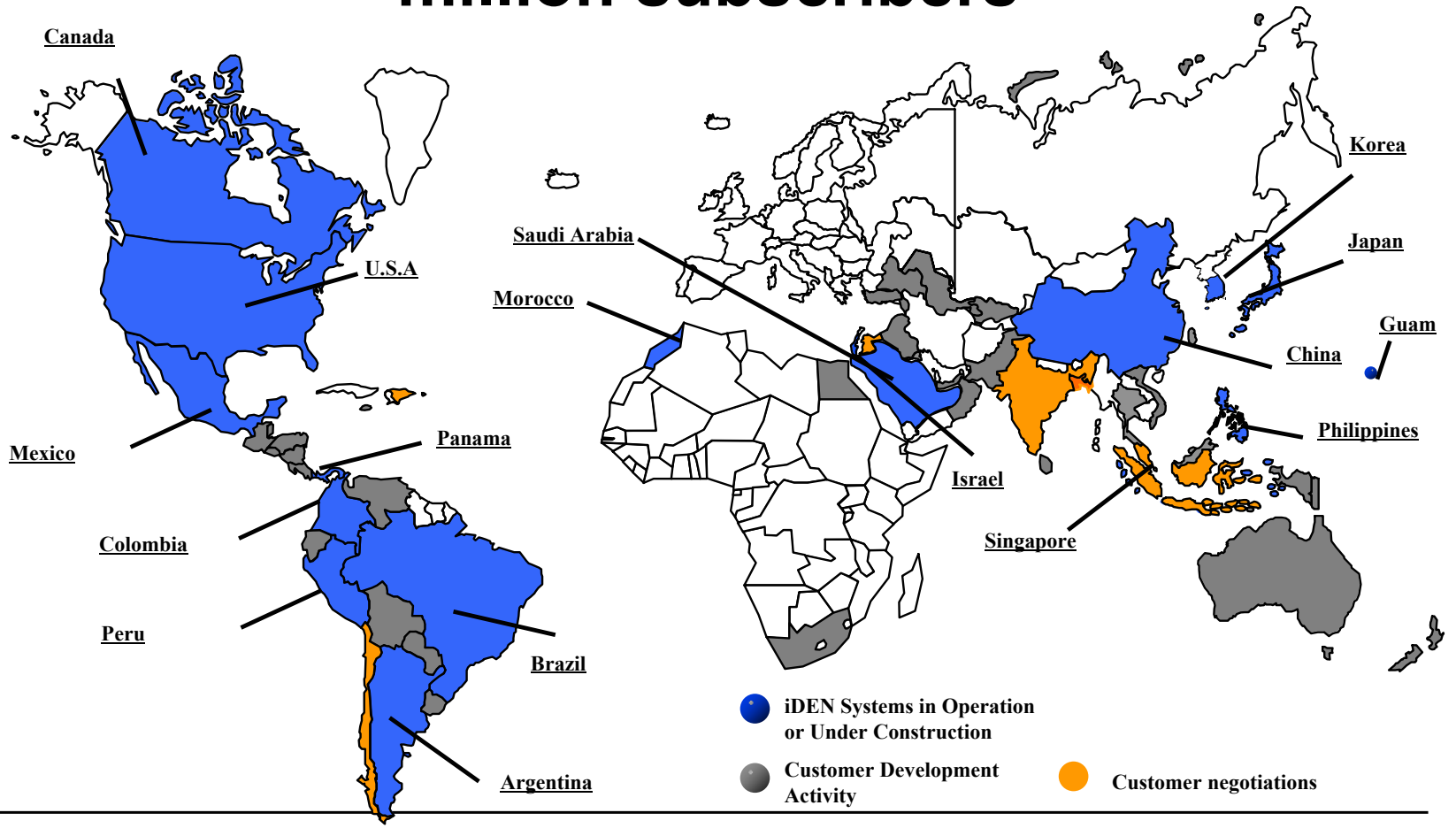
Topics Covered

- iDEN Background
- Pros and Cons of Public vs. Private Communications Systems
- iDEN Technical Attributes
  - Voice Security
  - Rugged, Low Cost Handsets
  - Integrated Java with Encryption
  - Integrated GPS
- Current and Upcoming Public Safety Models
- End-user perspective: US Forces Korea – Major Sean O'Mara

iDEN Background

- Technology developed in 1994 to allow multiple service devices in Specialized Mobile Radio (SMR) band
- Largest operator: US-based Nextel with 12M subscribers
- Networks in 14 other countries where SMR spectrum is available
- Technology continuously upgraded to support new features, higher data speeds

iDEN Worldwide Success- Over 16 million subscribers



MOTOROLA

intelligence everywhere™

Integrates ~~Four~~ Five Services Into a Single Device

Alphanumeric Messaging

iDEN

Data
- Circuit Switched
- Packet Switched
- J2ME

JAVA

Full Duplex Telephone Interconnect

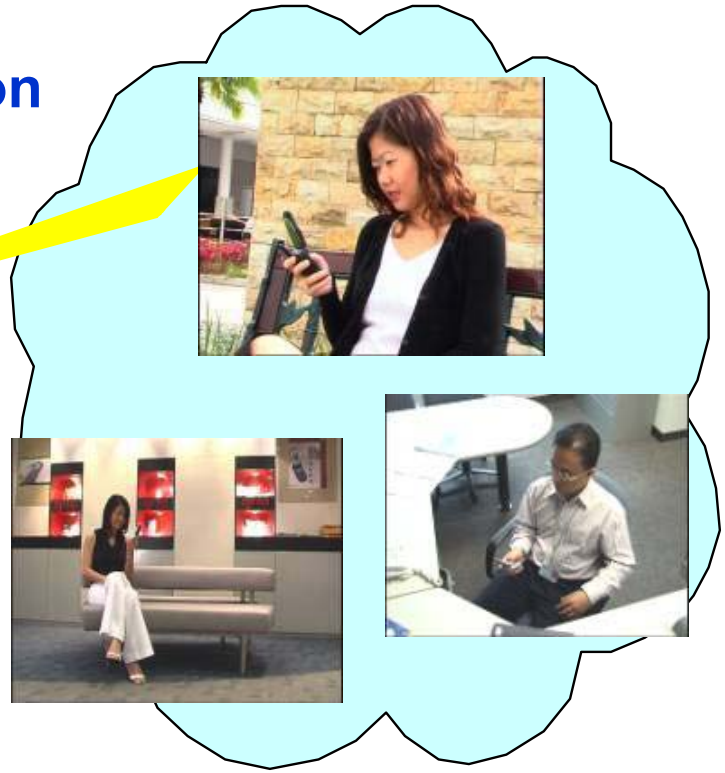
GPS

Direct Connect
- Private Call:
  - One to One
  - One to Many

Instant Private Communications

Private Call = 1 to 1 Communications

Call Alert = Discrete Notification



Instant Group Communications

Group Call = 1 to Many
Instant Conferencing
with a Work Group
At The Press Of A Button

Public vs. Private Communication Systems

Two Major Types of Public Services Communications Systems

- Traditional Private Land Mobile Radio (LMR) Network

- Use of Phones on a Commercial System (GSM, etc)

Model 1: Private Land Mobile Radio (LMR) System

Advantages:

- High degree of control
  - Coverage
  - Capacity
  - Cost
  - Priority Access on system
- One to one or broadcast capability
- Simplex (talk around) capability – independent of infrastructure
- Encryption
- Rugged Handsets

Disadvantages:

- Expensive – Large capital requirement
- Inflexible – System upgrades can be expensive and time-consuming
- Closed Group System – Limited Interoperability
- Annual maintenance costs
  - **Repairs**
  - **Personnel**
  - **Tower Rent (Real cost or opportunity cost)**
  - **Linking Circuits- T lines**
- Need to over engineer the system
  - **Back up power supplies**
  - **Redundant microwave**
- Long Planning, Funding, Implementation cycle
- If you err in planning you are stuck with the problem for the lifecycle

Model 2: Public Commercial System (GSM, CDMA)

Advantages:

- Connectivity to PSTN
- New technologies more easily deployed and less expensive
- Less resources needed to maintain system
- Form factor on subscriber devices
  - Smaller, lighter, lower-cost
- Limited up front capital costs
- Reoccurring costs can be budgeted with accuracy
- No hidden costs, and competition lowers total cost
- Higher data speeds both now and in the future

Disadvantages:

- Loss of control
  - –Dependent upon others to maintain your system
  - –Limited input re: coverage and capacity
- Current systems dependent on infrastructure
- Voice encryption not offered
- Vulnerable to Commercial Outages
- Lack of Instant Communications

iDEN's Unique Capabilities Fall Between the Two Models

- **Like a commercial cellular system iDEN has:**
  - **Large digital network coverage**
  - **Cellular Phone Mode**
  - **Wireless PCMCIA cards**
  - **SMS Messaging capability**
  - **J2ME Platform with SSL, crypto**
- **Like a private system, iDEN has:**
  - **Direct Connect – Instant Communications**
    - One to One
    - One to Many
  - **Secure internal communications**
  - **Interoperability – Can place dispatch calls to other agencies**
  - **Priority Access/Ruthless Preemption Capability**
    - **Emergency Call Capability**
  - **Ruggedized handsets available**

World Trade Center Example:

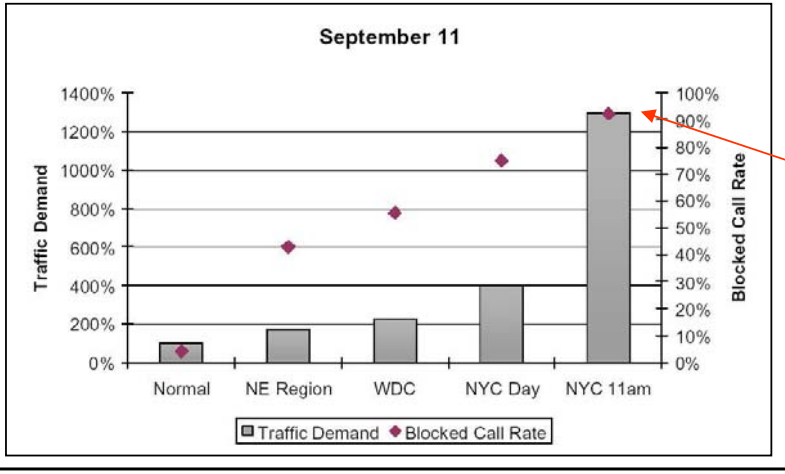
- **Private Systems:**
- Several federal agencies used WTC as primary transmit site for NY/NJ area, their systems were down. – still not up to pre 9/11 condition.
- FBI experienced 60% system degrading in lower Manhattan when a major telecommunications central office went offline knocking out system connectivity – 7 days and > $5 million dollars to restore.
- Paging services, ATM machines, and data services were all degraded in varying degrees – 10-15 days to restore.

- **Public Systems:**
- All commercial service providers dynamically increased capacity through the deployment of COW's in less than 12 hours.

Telecommunications is critical infrastructure and is a terrorist target.

World Trade Center Example

- Commercial Systems were affected as well, but in a different way
  - Initial attacks only destroyed or rendered inoperable 5 sites (among all carriers)
  - Congestion, PSTN failures, and Power Outages brought down 160 sites by evening
  - Call blocking reached 95% by 11AM
- iDEN Direct Connect was the only commercial service still functioning in the affected areas in the hours after the attacks
- Many agencies that used iDEN service distributed their units to FBI, police, firemen



95% Blocking during critical response time!

Source: CTIA Report to Network Reliability and Interoperability Council Oct 23, 2001

Why was iDEN service such a success?

- Dispatch service not connected to PSTN
  - All “internal” users
  - Not susceptible to switch overload from landline callers
- Supported Interoperability Across Agencies, Businesses
  - “Cross-Fleet” facilitated communications with non-traditional users
    - Red Cross, Salvation Army, the “Volunteer Corps”
    - Heavy equipment operators
    - Utility company personnel
- Able to add capacity as needed
  - COWs and BDAs added within hours after attacks

iDEN Has the Advantages of Both Models

iDEN combines the strengths of private LMR systems with the strengths of commercial systems to yield the best total system solution at less cost.

- Capacity – iDEN Operators add channels based on capacity needs
- Interoperability – iDEN's Direct Connect allows separate agencies to dispatch each other
- Instant Communication – Typical set up time: less than a second
- Secure Communications – iDEN dispatch calls are never converted to analog format
- Inherent redundancy in infrastructure – iDEN Carrier's networks all have redundant system elements
- Technology refresh comes faster and cheaper – New features every year
- Resistance to commercial PSTN failures – Direct Connect can run even when PSTN is down

- In the US, Nextel has partnered with Rudolph Giuliani Associates to Propose an iDEN solution for US Public Safety Interoperability:

http://www.giulianipartners.com/pr2.html

iDEN Technical Attributes

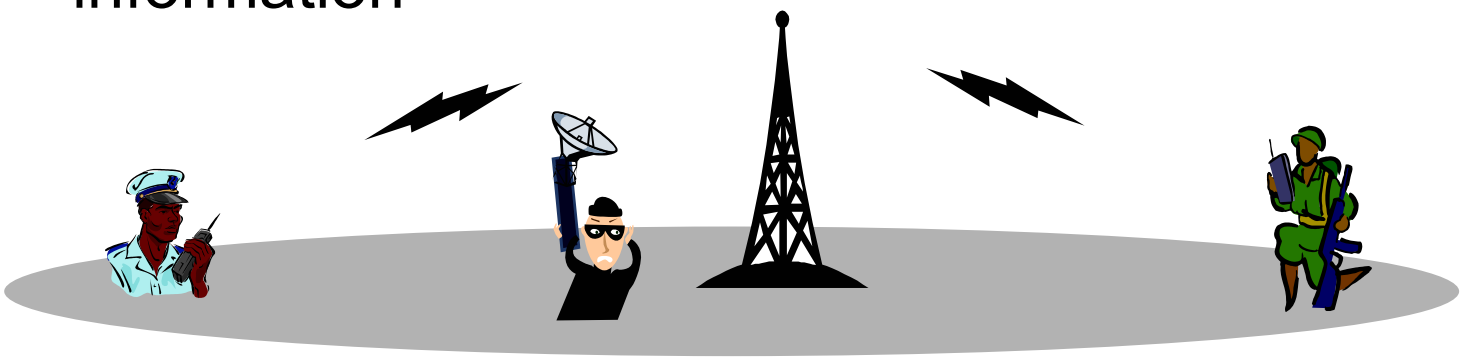
- Secure Voice
- Rugged, Low Cost Handsets
- Integrated Java with Encryption
- Integrated GPS

General Definition of Security

- Ability to prevent unauthorized individuals from listening in or obtaining data
- Various Methods and Implementations
  - Voice:
    - DES – Direct Encryption Standard
    - AES – Advanced Encryption Standard
    - Securenet –Analog Algorithm
  - Data
    - Symmetric vs. Asymmetric Crypto
- All Encryption Systems Can Be Broken
  - Given Sufficient Time & Resources

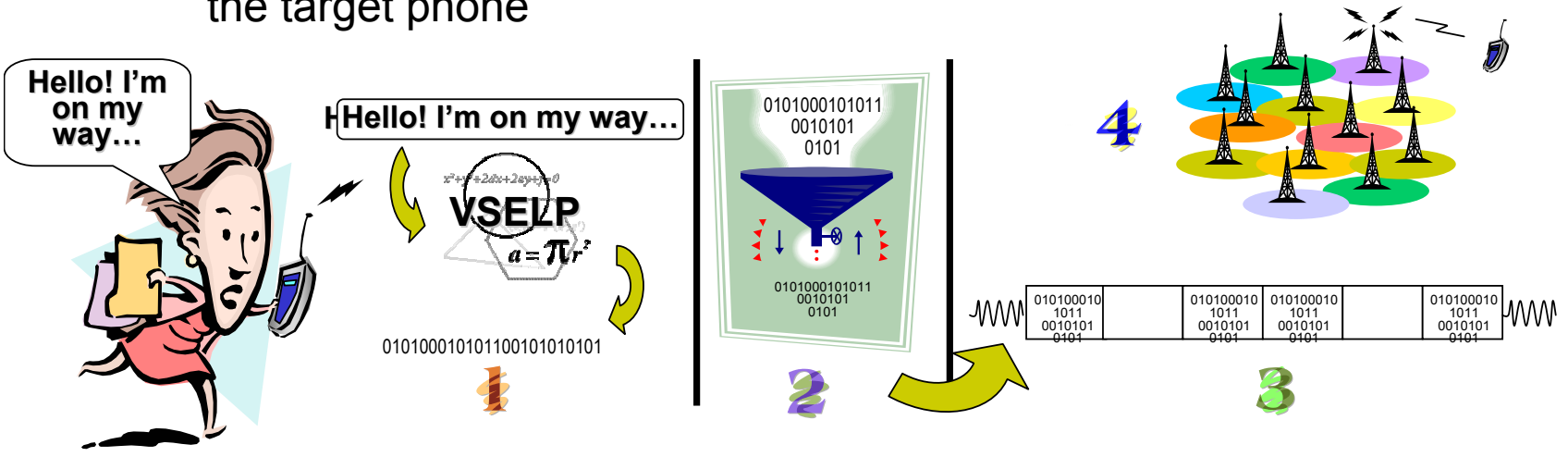
Why Security Needed for 2-Way

- Traditional transmissions were analog and “in-the-clear”
- Anyone with a scanner could listen in
- Very vulnerable and not good for sensitive information

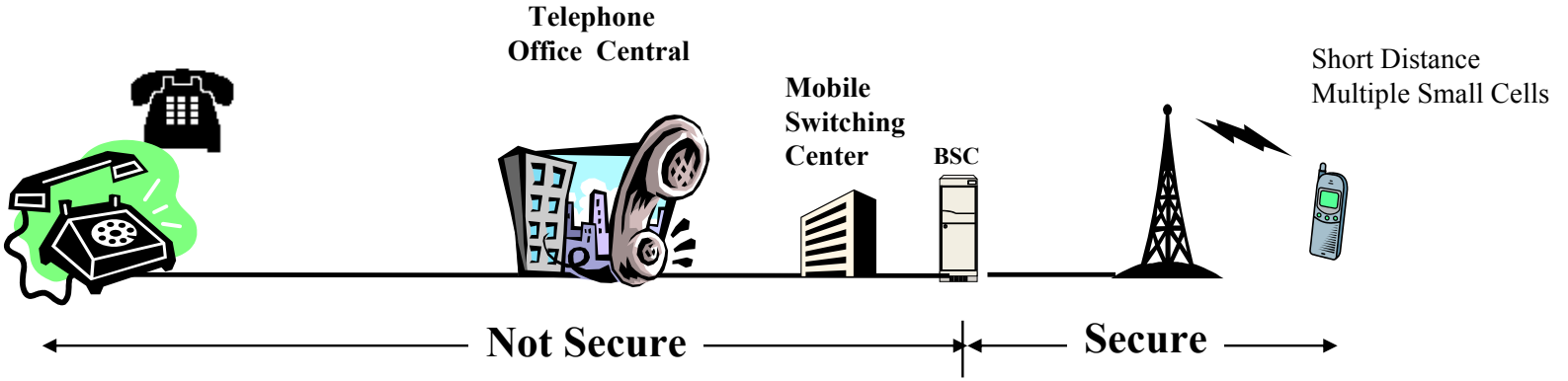


iDEN Resistance to Eavesdropping

1. iDEN is digitally encoded via a complex encoding scheme called VSELP (Vector Sum Enhanced Linear Prediction)
2. Once encoded, voice transmissions are compressed to one sixth their normal size
3. iDEN transmissions are broken into 15 msec bursts with specific time references that allow 6 conversations to share one channel
4. iDEN cell sites receive the data and pass it through the network to the target phone

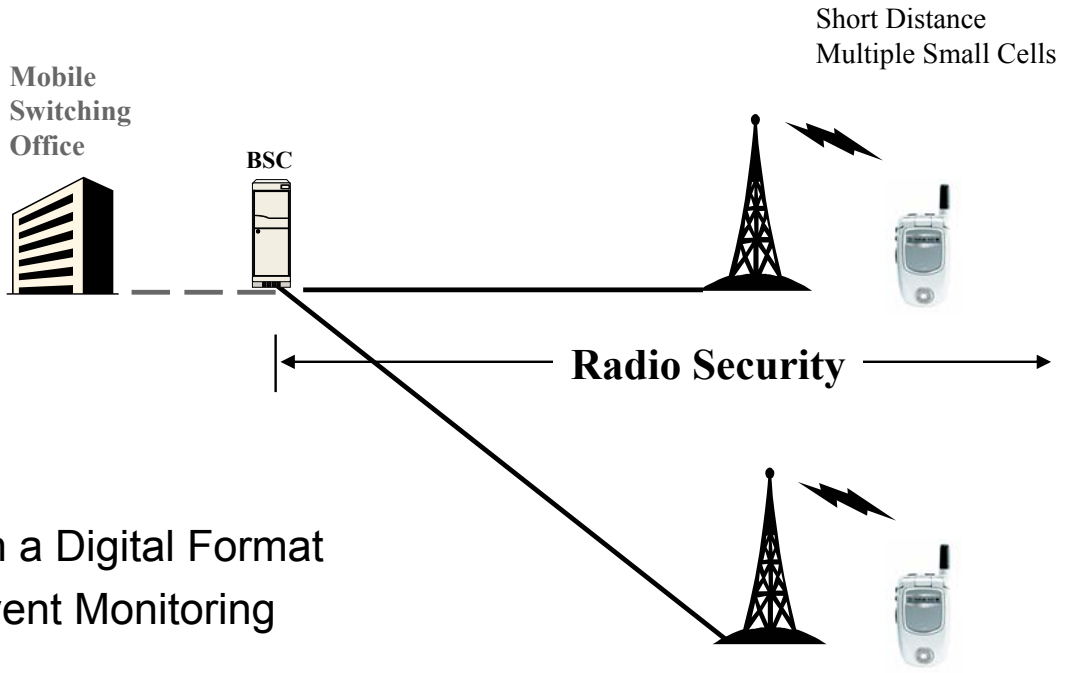


Telephone Interconnect Privacy



- Only Air Interface is Secured
  - Security Can Be Lost in the PSTN
- Small Cells Help Prevent Monitoring

Direct Connect Privacy



- Audio is Maintained in a Digital Format
- Small Cells Help Prevent Monitoring

“Breaking in” to iDEN

- RF
  - First, you’ve first got to find the right frequency in the 800 MHz band
- Digital Modulation
  - Next, you have to select the right timeslot (and align to it within a few microseconds)
  - Then, you must differentiate the four sub-channels and extract symbols according to the QAM (Quadrature Amplitude Modulation) scheme
- Handovers and Slot Shifts
  - While doing all this, you must hope the unit does not handover or switch slots within the cell, as often happens to improve voice quality
- Slot formatting
  - Assuming this is done, you must pull out the bits that handle voice traffic, and find a way to weed out the overhead bits, error correction bits, and slot preamble
- VSELP
  - Now that the entire bitstream has been extracted, it must be decoded from the VSELP format, which involves roughly 20 million arithmetic instructions per second to decompress
- Cloning Resistance
  - iDEN’s Ki, IMSI, TMSI, authentication procedures provide a layer of protection against theft-of-service or fraudulent use
  - Based on 128-bit GSM Authentication standard

iDEN Data Security

- iDEN Data is encrypted
  - Over-the-air encryption 64-bit “Vancouver” encryption
  - Application layer encryption
    - Phone.com browser: 128 bit RSA encryption
    - Application layer
      - J2ME: 128 bit, crypto toolkit APIs
      - Tethered application on PC
    - With App layer encryption, over-the-air piece is double encrypted
- Voice encryption is possible via J2ME application
  - Store & Forward voice packets. Limited to ~20 second bursts

iDEN Rugged Unit Specifications

Mil-Std 810F Tests

Test	Mil-Std-810F Test Procedure	Results/Remarks
Shock	Method 516.5 Procedure I, Functional Test for Ground Equipment & Procedure IV, 48" drop, 14 drops per radio	Passed
Vibration	Method 514.5 Procedure I, Cat 8, Aircraft Transport, Lo=0.30, fo=68Hz, 1 hr per axis 15-2000 Hz	Passed
Dust	Method 510.4 Procedure I, Blowing Dust, 900 ft/min, 6 hours at 23°C, 6 hours at 60°C	Passed
High Temperature	Method 501.4 Procedure I, seven cycles, climate category - Hot & Procedure II, +60°C,2 hours	Passed
Low Temperature	Method 502.4 Procedure I, -45°C, 24 hours & Procedure II, -10°C, 2hours	Passed
Low Pressure	Method 500.4 Procedure II, 15,000 ft., 1 hour	Passed
Solar Radiation	Method 505.4 Procedure I, Diurnal cycle A1, 3 cycles	Passed
Humidity	Method 507.4 Procedure I, ten 24 hr cycles	Passed
Temperature Shock	Method 503.4 Procedure I, +85°C to -40°C, 4 hrs at temp, 3 cycles	Passed
Salt Fog	Method 509.4 Procedure I	Passed
Blowing Rain	Method 506.4 Conditions: Rainfall Rate: 6 in/hr, Five Exposure Surfaces, No Preheat, Ambient water temperature, Wind Velocity 40 mph, Exposure time, 30 minutes per face	Passed

Java (J2ME) and the Mobile Handset

Applications written in Java

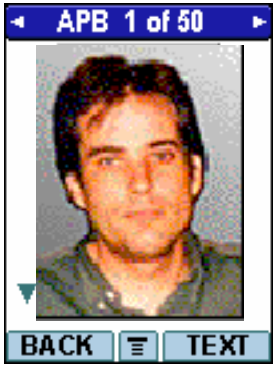
Write the application once... Run Across a whole range of devices and operating systems

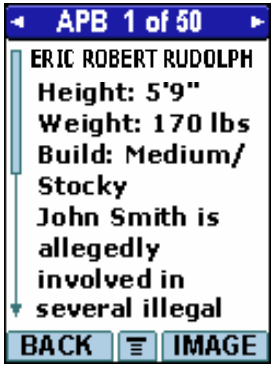
- Standards Based
- Vertical Applications
- Robust API Set (Access to major handset functions)
- Personalization
- Local execution
- Security & Crypto APIs (including AES)

Visual *APB*™ Plus

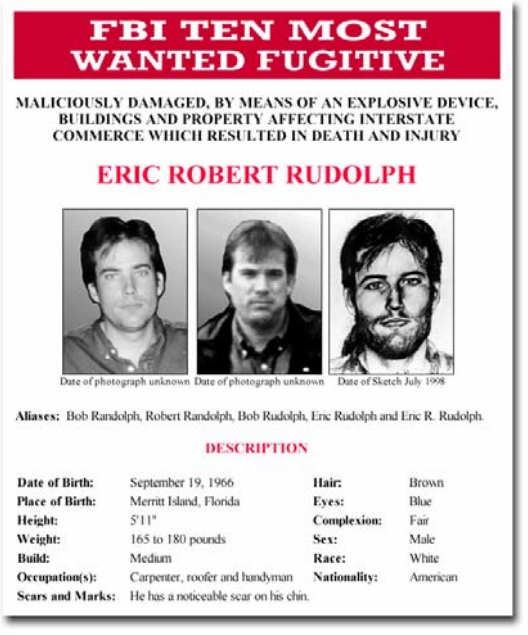
Imaging Broadcast & Messaging Solution

- Secure - Suspect Identification and Messaging Application
- Immediate “Global” Wireless Updates
- End-to-End - RC4 Security
- Broadcast delivery of full-color digital images and text
- Situation Specific Information





Wireless Identify Application



FBI TEN MOST WANTED FUGITIVE

MALICIOUSLY DAMAGED, BY MEANS OF AN EXPLOSIVE DEVICE, BUILDINGS AND PROPERTY AFFECTING INTERSTATE COMMERCE WHICH RESULTED IN DEATH AND INJURY

ERIC ROBERT RUDOLPH

Date of photograph unknown Date of photograph unknown Date of Sketch July 1998

Aliases: Bob Randolph, Robert Randolph, Bob Rudolph, Eric Rudolph and Eric R. Rudolph

DESCRIPTION

Date of Birth:	September 19, 1966	**Hair:**	Brown
Place of Birth:	Merritt Island, Florida	**Eyes:**	Blue
Height:	5'11"	**Complexion:**	Fair
Weight:	165 to 180 pounds	**Sex:**	Male
Build:	Medium	**Race:**	White
Occupation(s):	Carpenter, roofer and handyman	**Nationality:**	American
Scars and Marks:	He has a noticeable scar on his chin.		

Original paper-based and Web-based system

Developer Solution

Facial Recognition and Identification

- Remote access to security databases for immediate user identification
- Retrieve images and updated address information

Mobile Location Services

Information

- Where am I
- Where is…
- Vehicle traffic
- Driving Direction

Entertainment

- Gaming

Cut Response Time

- Send Closest Agent

Instant Messaging

- Locate Co-Worker

i730 w/ GPS

Emergency

- E911/E112
- Roadside Assistance

Tracking/Navigation

- Fleet Management
- People Finding
- Asset Tracking
- Vehicle Navigation

Network Optimization

- Location Sensitive Billing
- Network Planning

Integrated GPS

- Network Independent
  - Does not require network coverage to obtain a Lat/Long coordinate fix
  - Can continue to record position information until unit returns to coverage
- Access to unit's position
  - Units can be programmed to always respond, never respond, or ask the user's permission (case by case basis)
  - Override can be set for emergency situations
- Accuracy within 20-50m
  - Units in coverage receive assist data from network
  - Improves accuracy and time to first fix (TTFF)

iDEN Subscriber Handset Portfolio

New Products

i730 – Consumer Model

- Mid-Hi Tier Product
- Color 130x130 display
- Outer CLI display
- GPS
- Enhanced Java
- 16MB RAM
- Size Reduction from i95cl
- Longer battery life
- Improved User Interface

i305 – Entry Level

- Basic Entry Level Products
- Mono 96 x 64 display
- Condor Ergonomics
- Mil Spec
- GPS
- No Java
- 4MB RAM

Public Safety Handsets

Conch Plus

- Adds MotoTalk (900 ISM Band*) to Conch (i305)
- Different Housing
- Mil Spec 810 C,D, & E
- Access Class (ACC)
- Targeted availability: May 04

Conch Pro

- MotoTalk (900 ISM Band*)
- Mil Spec 810 C,D, & E
- AFU Feature Set
  - Emergency Group Call
  - Isolated Site Operation
  - Simultaneous Group Scan
  - Instant Status Message
- Color Display 96x65
- Java Support
- Access Class (Load Shedding)
- Rugged Accessory Connector
- Fixed Antenna
- Targeted availability: May 04

Conch Pro II

- MotoTalk (900 ISM Band*)
- Mil Spec 810 C,D, & E
- AFU Feature Set
  - Same as Conch Pro
- Large Color Display 130x130
- Java Support
- Access Class (Load Shedding)
- Rugged Accessory Connector
- Fixed Antenna
- Top Mounted Emergency Button
- Voice Encryption
- Night-Vision Goggle Support
- Targeted availability: 1Q 05

* 900 MHz ISM Band (902-928 MHz) not currently available in some markets

Upcoming iDEN Technology Enhancements

- WiDEN – 4x data speed improvement: 132kbps RF channel – End 2004

- Upcoming iDEN Dispatch Feature Enhancements:
  - Selectable Dynamic Group Call
  - Push-to-View
  - iExchange – vCard transfer

END OF PRESENTATION