Iridium Security

Datalink Users Forum

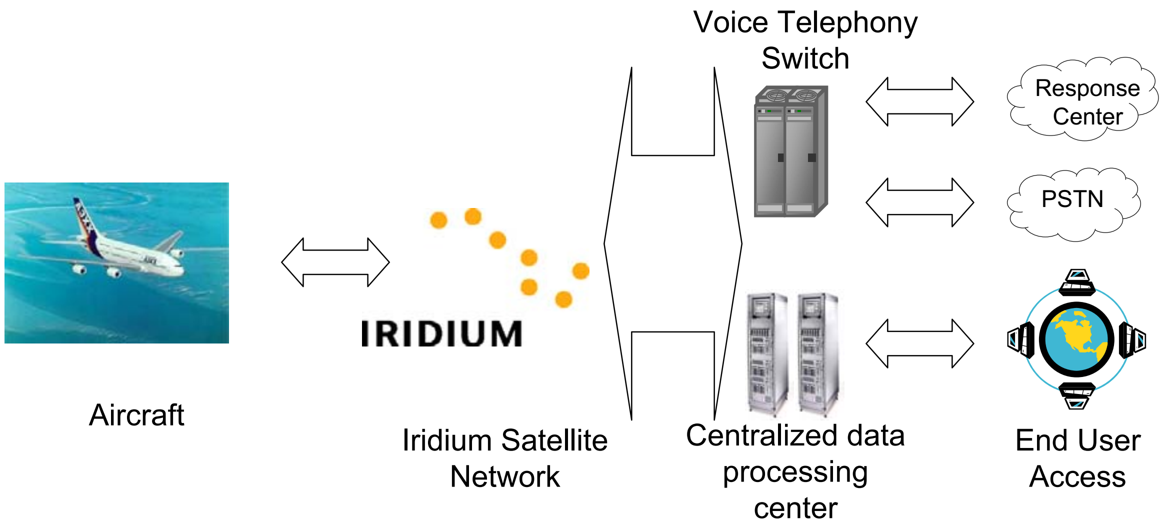
David Wigglesworth
Iridium Satellite LLC
07 Feb 07

Contents

- Inherent Network Security
- Solution Security

Inherent Network Security

Generic Solution Architecture



Voice Telephony Switch

Response Center

PSTN

Aircraft

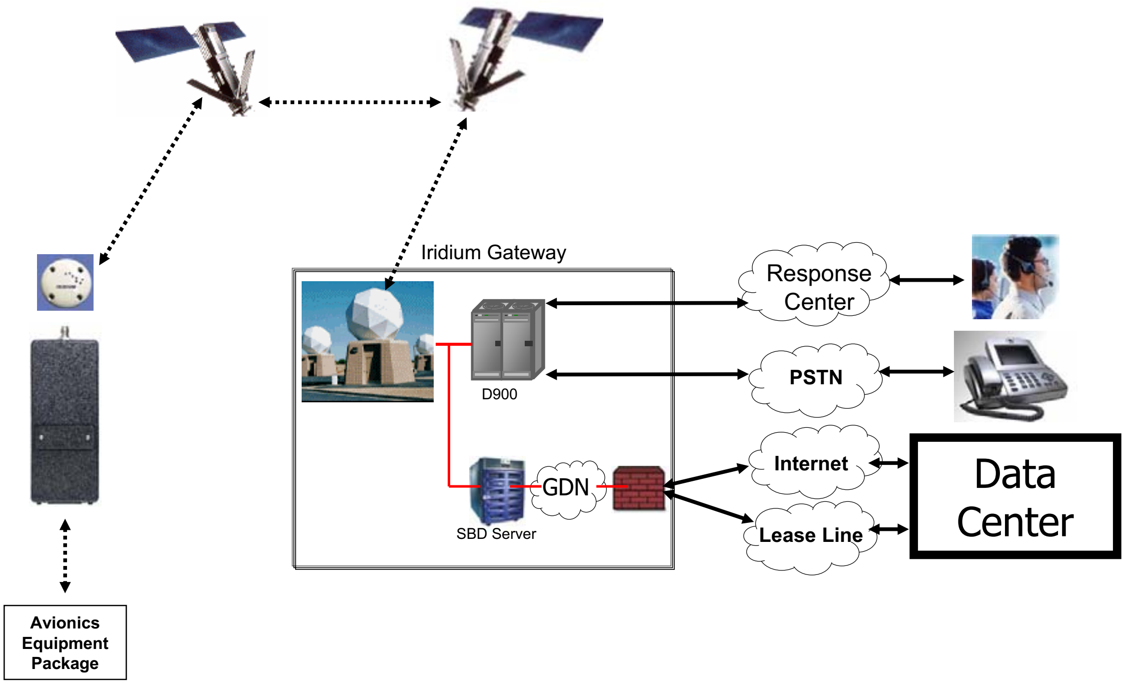
IRIDIUM

Iridium Satellite Network

Centralized data processing center

End User Access

Functional Network Architecture



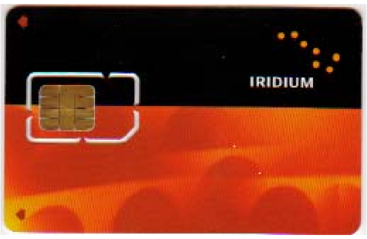
Introduction

The Iridium System supports the GSM-specified algorithm A3 for authentication security.

The table below summarizes the security features explicitly designed into the Iridium system.

Authentication	A3 (128-bit Key)
Equipment Anti-Theft Validation	Global EIR
Anonymity (User location confidentiality)	TMSI based
Signaling Message Confidentiality	Not Available
Voice Privacy	Not Available
User Fax/Data Confidentiality	Not Available
User Verification	SIM-based PIN

Authentication



- The Iridium System supports the GSM-specified algorithm A3 for authentication security in SIM based subscriber equipment
- The Iridium authentication process is adapted without change directly from the GSM specifications.
- The GSM algorithm A3 is used to encrypt authentication information transmitted over the air interface.
  - Authentication encryption
  - Designed to prevent ISU cloning fraud
  - GSM encryption algorithm A3 is executed on SIM card to generate Signed Result (SRES) response based on the following inputs
    - Secret Ki parameter stored in SIM card
    - RAND parameter supplied by network

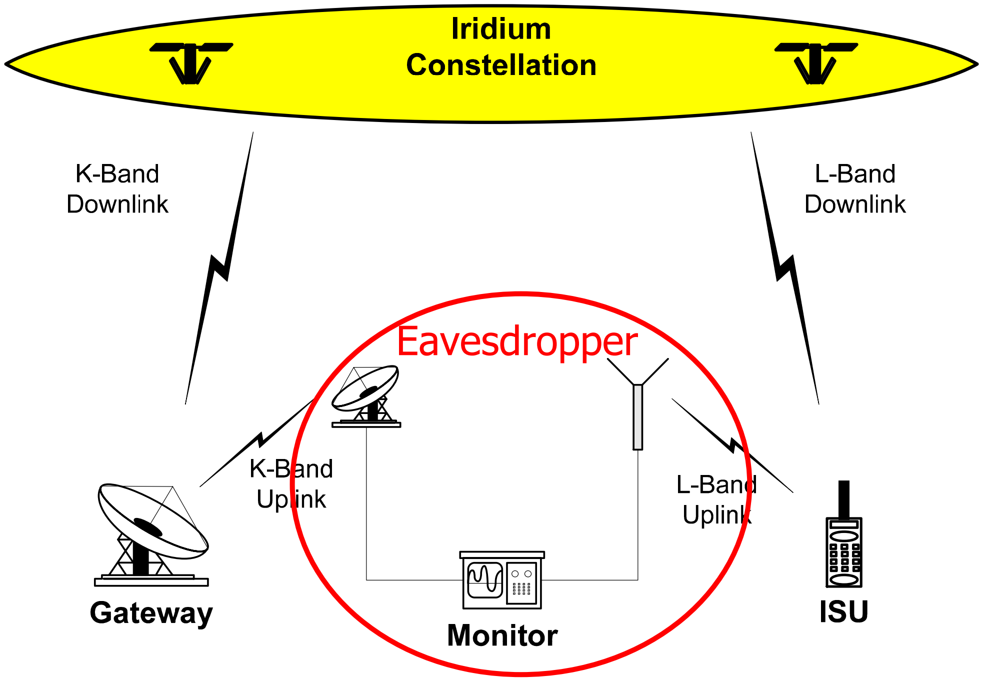
Hardware/Equipment Validation

- EIR - Equipment Identity Register
  - Simply a “white list” and “black list”
- The EIR is a database
- When a ISU requests services from the network its IMEI (International Mobile Equipment Identity) is checked against the EIR to assess which category it falls into.
- Black-listed ISUs are not allowed to access the network:
  - Those reported stolen or
  - Whose operation on the network will adversely affect the network
- White-listed ISUs are those that are permitted to access the network.

Iridium Channel Security

- Iridium voice, data, and signaling channels are afforded some security by the limited distribution of the air interface and feederlink interface specifications.
- The Iridium Air Interface Specification is made available only to Iridium Subscriber Unit (ISU) manufacturers.
  - Iridium Satellite LLC is the sole ISU manufacturer
- Feederlink interface specifications are not distributed outside of Motorola.
- Opportunities for surreptitious monitoring of Iridium bearer channels exist. An eavesdropper could, in principle, monitor:
  - L-Band Channels
    - Uplink, from ISU to Space Vehicle (SV)
    - Downlink, from SV to ISU
  - K-Band Channels
  - Uplink, from gateway to Space Vehicle (SV)
  - Downlink, from SV to gateway

Iridium Link Monitoring Opportunities



L-Band Channel Security

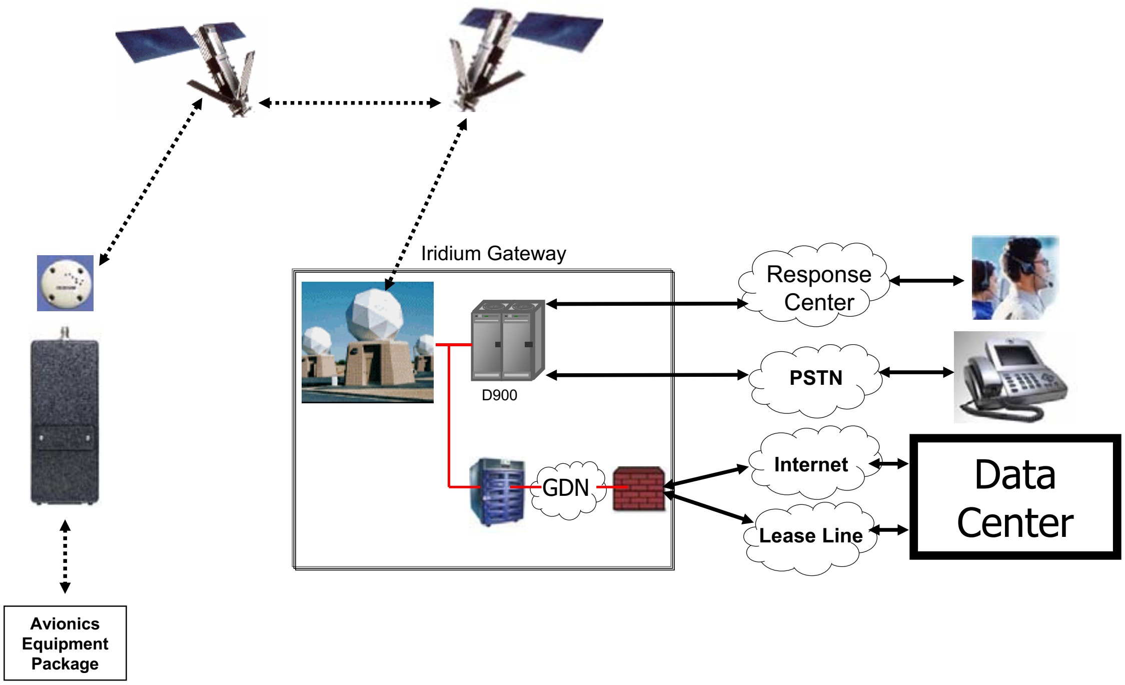
- To monitor an L-band channel,
  - Located within the transmit range of the ISU being monitored (10 to 30 km)
  - ISU downlink L-Band transmissions could be received over a much wider area but within the coverage area of a common beam
- The complexity of the Iridium air interface makes the challenge of developing an Iridium L-Band monitoring device very difficult and probably beyond the reach of all but the most determined adversaries.
- Among the complications are
  - Large, continually changing Doppler shifts
  - Frequent inter-beam and inter-SV handoffs
  - Time-division multiplexed burst mode channels
  - Complicated modulation, interleaving and coding

K-Band Channel Security

- To monitor a K-band feederlink channel
  - Sophisticated monitoring device located in the general proximity of an Iridium gateway.
  - High-gain antenna capable of tracking SVs as they move from horizon to horizon.
- Complexity of feederlink interface poses a formidable technical challenge for prospective eavesdroppers.
- Cost of the monitoring device alone would be a strong deterrent.
- Among the technical complications are
  - Large, continually changing Doppler shifts
  - High capacity, 3.072 Mbps channels
  - High-gain tracking antenna required
  - Must reacquire new SV every 10 minutes

Solution Security

Functional Network Architecture



Iridium Gateway

D900

GDN

Response Center

PSTN

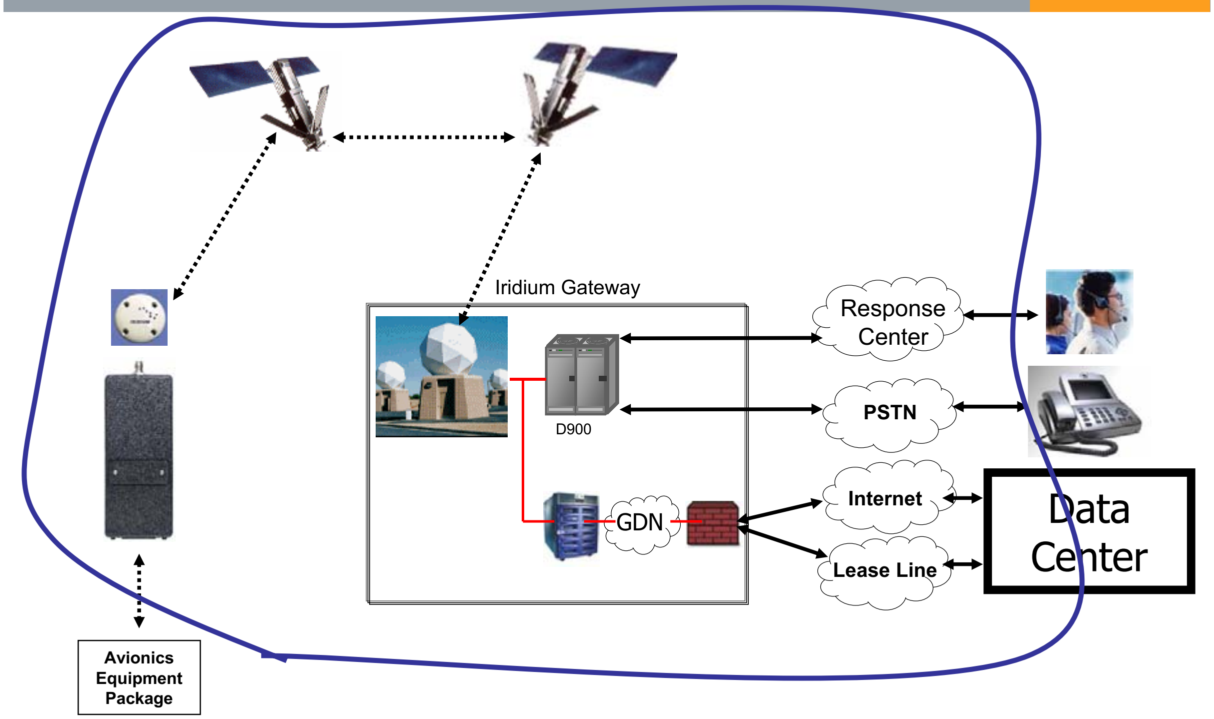
Internet

Lease Line

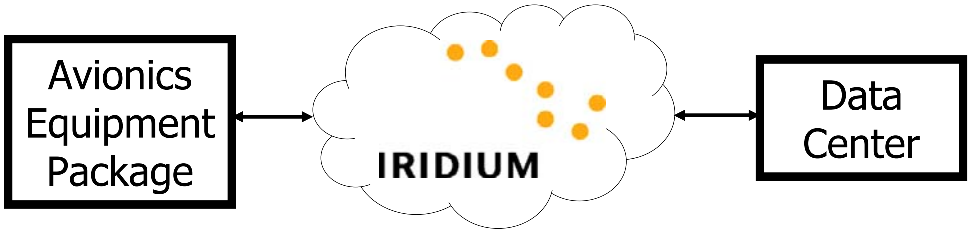
Data Center

Avionics Equipment Package

Functional Network Architecture



Solution Security



- Iridium is the “pipe”
- End to end security/authentication is required in the application
- Consideration should be given by the application designer how applications residing on aircraft or at data centers validate received/sent messages
- Connectivity to/from Iridium is available via VPN and/or leased line

Questions?

David Wigglesworth
Director – Data Services

Iridium Satellite LLC
David.Wigglesworth@iridium.com
+1-301-571-6242