Space and Missile Systems Center

Over-the-Air Distribution (OTAD) Update

Maj Scott Tyley, SMC/GPEP
29 Apr 15
Informational Briefing

• OTAD Overview
• Background
• Benefits
• Events
• OTAD Demo
• Summary
• OTAD/OTAR are alternative methods of key distribution
  – OTAD Next black key sent to user via the GPS navigation message
  – OTAR Superset of OTAD key sent via the navigation message
• Receiver must be on and have a good daily key
• If receiver is off or out of keys user obtains next key from COMSEC custodian
OTAR/OTAD Background

• Many users rely on OTAD for distribution of cryptokeys
  – DAGR S/W update released to take full advantage of OTAD and mission constellation operations
  – 4+ years of successful US OTAD broadcasts

• Mission constellations allow simultaneous broadcast of multiple OTAD messages
  – The SAASM Mission Planning System (SMPS) at the JSpOC performs constellation optimization and assigns OTAR/OTAD keys to be broadcast from each SV
Benefits of OTAD

• SAASM-enabled Over-The-Air cryptokey distribution provides a means to keep users keyed and protected
  – Receivers are significantly more resilient to attack when they are keyed and operating with the PPS
  – More reliable cryptography distribution for GPS PPS to coalition warfighters
  – Decreased COMSEC maintenance burden on coalition warfighters
    • Re-key time decreased to 12.5 minutes once a month with no need for paper tape, COMSEC storage, or physical touch
  – Mission constellations enables system to support US and Allied users simultaneously
OTAD/R Events

- 2005 - 4 phases of OTAR testing
- 2009 - Transition Exercises 4 and 5 (Oct-Dec)
  - (Test Key) OTAR/OTAD capabilities were tested
- 2010 - Transition Exercise 7 (Oct-Nov)
  - On-orbit OTAD broadcast of a coalition key on all SVs for approximately 28 days
- 2011 - Start of on-orbit operational US OTAD broadcasts on all SVs continuously (Mar - present)
- 2011 - Multi-Service Operational Test & Eval (Aug)
- 2012 - AEP v5.8 deployed (Jun)
- 2013 - On-Orbit Mission Constellation Test (Feb-Mar)
- 2014 - Allied OTAD Demo
- 2014 - Block II EP IOC (Oct)
- 2015 - Allied Operational OTAD Broadcasts
- 2015 - SMPS version 5a install at JSpOC (Nov)
OTAD
Demonstration Overview

STRATCOM
Approved OTAD Country List

JFCC-Space
OTAD Schedule

JSpOC
ICD-GPS-215 Compliant Joint SAASM Supplement

MCS
SV Command & Control (GPS GAs)
Signal Monitoring (GPS Monitor Stations)

Country 1
Country 2
Country 3
Country 4

Space Support Requests
Effects Monitoring Local/Global (NGA)

Mission Constellations
# Notional OTAD Broadcast Schedule

<table>
<thead>
<tr>
<th>Mission Constellation 1</th>
<th>Day 1</th>
<th>Day 2</th>
<th>Day 3</th>
<th>Day 4</th>
<th>Day 5</th>
<th>Day 6</th>
<th>Day 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>US OTAD</td>
<td>Country 1</td>
<td></td>
<td>Country 1</td>
<td></td>
<td>Country 1</td>
<td></td>
<td>Country 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mission Constellation 2</th>
<th>Day 1</th>
<th>Day 2</th>
<th>Day 3</th>
<th>Day 4</th>
<th>Day 5</th>
<th>Day 6</th>
<th>Day 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allied OTAD</td>
<td>Coalition</td>
<td>Country 1</td>
<td>Country 2</td>
<td>Coalition</td>
<td></td>
<td>Country 2</td>
<td>Coalition</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mission Constellation 3</th>
<th>Day 1</th>
<th>Day 2</th>
<th>Day 3</th>
<th>Day 4</th>
<th>Day 5</th>
<th>Day 6</th>
<th>Day 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allied OTAD</td>
<td>Coalition</td>
<td></td>
<td>Coalition</td>
<td></td>
<td>Coalition</td>
<td></td>
<td>Coalition</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mission Constellation 4</th>
<th>Day 1</th>
<th>Day 2</th>
<th>Day 3</th>
<th>Day 4</th>
<th>Day 5</th>
<th>Day 6</th>
<th>Day 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTAR Reserved</td>
<td>Reserved</td>
<td>Reserved</td>
<td>Reserved</td>
<td>Reserved</td>
<td>Reserved</td>
<td>Reserved</td>
<td>Reserved</td>
</tr>
</tbody>
</table>

*Keys broadcast to multiple users worldwide simultaneously*
Summary

• OTAD ensures warfighter remains keyed and protected
  – More secure and flexible cryptography
  – Reduced crypto key management burden
  – Receivers more resilient to attack
  – Mission constellations enables GPS to support US and Allied users simultaneously