Defense Systems
Information Analysis Center

# DSIAC TECHNICAL INQUIRY (TI) RESPONSE REPORT

## Miniature Cryptographic Appliqué for Identification Friend or Foe (IFF) Transponders

**Report Number:**
DSIAC-2019-1031
**Completed October 2018**

**DSIAC** is a Department of Defense
Information Analysis Center

**MAIN OFFICE**
4695 Millennium Drive
Belcamp, MD 21017-1505
443-360-4600

**REPORT PREPARED BY:**
Scott E. Armistead

# ABOUT DSIAC

The Defense Systems Information Analysis Center (DSIAC) is a U.S. Department of Defense information analysis center sponsored by the Defense Technical Information Center. DSIAC is operated by SURVICE Engineering Company under contract FA8075-14-D-0001.

DSIAC serves as the national clearinghouse for worldwide scientific and technical information for weapon systems; survivability and vulnerability; reliability, maintainability, quality, supportability, and interoperability; advanced materials; military sensing; autonomous systems; energetics; directed energy; and non-lethal weapons. We collect, analyze, synthesize, and disseminate related technical information and data for each of these focus areas.

A chief service of DSIAC is free technical inquiry (TI) research, limited to 4 research hours per inquiry. This TI response report summarizes the research findings of one such inquiry. For more information about DSIAC and our TI service, please visit www.DSIAC.org.

# ABSTRACT

The Defense Systems Information Analysis Center (DSIAC) received a technical inquiry requesting small size, weight, and power cryptographic devices for Mode-5 transponders and radios in small unmanned aerial vehicle applications. DSIAC searched open sources for commercially available systems as well as the Small Business Technology Transfer/Small Business Innovation Research database for developmental efforts. The results were compiled into a matrix of systems and their characteristics allowing comparison by size, volume, and weight, and were delivered to the inquirer.

# Contents

# 1.0 TI Request

## 1.1 INQUIRY

What miniaturized cryptographic devices are available for transponder and radio applications in small unmanned aerial vehicles (UAVs)?

## 1.2 DESCRIPTION

Information was requested on small size, weight, and power (SWaP) cryptographic devices, such as miniaturized KIV-77 or KIV-78 equivalents, for Mode-5 Identification Friend or Foe (IFF) transponders and radios for use in small UAV applications. The mainly interest was in stand-alone devices versus cryptographic devices that are integrated into the IFF transponder itself.

# 2.0 TI Response

The Defense Systems Information Analysis Center (DSIAC) staff searched open sources including the Small Business Technology Transfer/Small Business Innovation Research (STTR/SBIR) database for information on existing or developmental programs to develop miniature IFF cryptographic devices. The focus of the search was on separate cryptographic appliqués; however, small form-factor integrated systems were also catalogued. Table 1 lists information on the systems identified in the search.

The inquiry referenced 2 cryptographic appliqués produced by General Dynamics Mission Systems (GD MS) and Raytheon [1, 2]. DSIAC contacted GD MS to request information on their Mini IFF Crypto Applique (MICA) because it seemed particularly well suited as it was advertised as being very small (i.e., 5.5 cubic inches, 5.0 oz). GD MS also recommended their recently developed KIV-78 system, which is significantly larger (33.6 cubic inches, 24 oz) [3, 4]. The company provided DSIAC with the contact information of the IFF Engineering Project Leader [5].

DSIAC found information on three other developmental efforts and one production effort for small form-factor IFF cryptographic devices, including the following:

- Air Force Life Cycle Management Center (AFLCMC) Cryptologic and Cyber Systems Division.
    - AFLCMC has developed a “Mini Crypto” device. In 2017, they noted the development of a low-power (400 mW), self-contained, encryption engine with a small design (approximately the size of a “cracker” with an estimated volume of approximately 0.5 cubic inches). Implementation requires a chip at both the transmitter and receiver end as the system establishes its own crypto key between sender and receiver [6].
- Intelligent Automation, Inc. (IAI).
    - IAI was awarded Navy SBIR Phase I and II contracts to develop a miniature (3.5 cubic inches) IFF ADS-B Mode 1 through 5 transponder with single-chip, System-on-Chip (SOC)-based crypto system architecture [7].
    - Currently, IAI is producing a Micro IFF Transponder (MIFFT) with “embedded crypto” that is fairly small (6.9 cubic inches, 10.0 oz) with an embedded AIMS 04-900 compliant cryptographic engine with Mode 5 support [8, 9].
- Sagetech Corporation.
    - Sagetech was awarded Navy SBIR Phase I and II contracts to develop a small ADS-B IFF transponder and associated “micro-crypto” appliqué (5.5 cubic inches, 5.0 oz) [10].

**Table 1: Catalogued Small Identification Friend or Foe (IFF) Transponder Cryptographic Devices [1-4, 6-15]**

| Manufacturer | Crypto Appliqué Name | Modes Supported | Reference No. | Dimensions (inches) | | | Volume (cubic inches) | Weight (ounces) | Notes |
|---|---|---|---|---|---|---|---|---|---|
| Air Force Life Cycle Management Center (AFLCMC) Cryptologic and Cyber System Division | Mini Crypto | —— | [6] | 2.00 | 2.00 | 0.13 | 0.5 | —— | In 2017, AFLCMC noted the development of a self-contained encryption engine with a small (approximately the size of a cracker) low-power (400 mW) design. It requires a chip at both the transmitter and receiver end as the system establishes its own key between sender and receiver. Size is estimated based on standard soda cracker comparison noted in the article [6]. |
| Intelligent Automation, Inc. (IAI) | Navy Small Business Innovation Research (SBIR) 2014.2, Topic N142-102 | Modes 1, 2, 3, 4, 5 | [7] | —— | —— | —— | 3.5 | —— | IAI proposed to develop miniature IFF ADS-B Mode 1 through 5 transponder with 3.5-cubic-inch volume and single-chip, System-on-Chip (SOC) based crypto system architecture. They were awarded Phases I and II. |

| Manufacturer | Crypto Appliqué Name | Modes Supported | Reference No. | Dimensions (inches) | | | Volume (cubic inches) | Weight (ounces) | Notes |
|---|---|---|---|---|---|---|---|---|---|
| Sagetech Corporation | Navy SBIR FY2014.2, Topic N142-102, Micro Identification of Friend of Foe (IFF) | —— | [10] | —— | —— | —— | 5.5 | 5.0 | Sagetech proposed the development of a 150-gm ADS-B IFF transponder and associated micro-crypto applique with a weight of 5 oz and volume of 5.5 cubic inches. Sagetech was awarded Phases I and II. (The Sagetech website still shows the MX family of micro transponders as using the KIV-77 external crypto appliqué). |
| IAI | Micro IFF Transponder (MIFFT) - embedded crypto | Modes 1, 2, 3/A, C, 5, S | [8, 9] | 2.50 | 2.50 | 1.10 | 6.9 | 10.0 | MIFFT is AIMS 03-1000B Annex G compliant with embedded AIMS 04-900 compliant crypto engine for Mode 5 support. National Security Agency (NSA) certification is in progress [8]. |
| General Dynamics Mission Systems (GD MS) | Mini IFF Crypto Applique (MICA) | Mark IIA, Modes 4 and 5 | [1, 2] | 3.00 | 4.50 | 1.10 | 14.9 | 19.0 | None. |
| Raytheon | KIV-77 Common IFF Appliqué Crypto Computer | Mark IIA, Modes 4 and 5 | [11] | 3.50 | 4.25 | 1.00 | 14.9 | 16.0 | None. |
| BAE Systems | KIV-6 Mark XI IIFF Crypto | Mode 4 | [12] | 3.40 | 2.05 | 4.68 | 32.6 | 32.0 | None. |

| Manufacturer | Crypto Appliqué Name | Modes Supported | Reference No. | Dimensions (inches) | | | Volume (cubic inches) | Weight (ounces) | Notes |
|---|---|---|---|---|---|---|---|---|---|
| GD MS | KIV-78 — Mode 4/Mode 5 IFF Crypto Appliqué | Mark IIA, Modes 4 and 5 | [3, 4] | 3.40 | 4.70 | 2.10 | 33.6 | 24.0 | KIV-78 is a form-factor replacement for KIV-6; used by the AN/APX-111, AN/APX-113(V), and AN/APX-125(V) Combined Interrogator/Transponders (CITs) in F-16, JASDF F-2, and NATO MiG-29; anti-submarine warfare (ASW) rotary wing aircraft such as S-61 and sine versions of F-15 and F/A-18 [3]. |
| Thales Group | TSK 4000 IFF Cryptographic Unit | National Secure Mode | [13] | 1.38 | 5.79 | 4.96 | 39.6 | 35.3 | None. |
| Hensoldt | QRTKxNG IFF Mode 4/Mode 5 Crypto Computer | Mark IIA, Modes 4 and 5 | [14, 15] | 7.87 | 1.77 | 5.00 | 69.6 | 35.3 | None. |

# REFERENCES

[1] GD MS. "Mini IFF Crypto Applique (MICA)." https://gdmissionsystems.com/products/encryption/embedded-encryption/mini-iff-crypto-applique, accessed October 2018.

[2] GD MS. "Reduced Form Factor IFF Cryptographic Appliqué." https://gdmissionsystems.com/-/media/General-Dynamics/Cyber-and-Electronic-Warfare-Systems/PDF/Spec-Sheets/cyber-mini-iff-crypto-applique-mica-datasheet.ashx?la=en&hash=DD178AE4EA6BF505F9F789480BB4EE4C9309BA66, 2015.

[3] GD MS. "KIV-78 – Mode 4/Mode 5 IFF Crypto Appliqué." https://gdmissionsystems.com/products/encryption/embedded-encryption/kiv-78-mode-5-mode-5-iff-crypto-applique, accessed October 2018.

[4] GD MS. "KIV-78 – Mode 4/Mode 5 IFF Crypto Appliqué." Brochure, https://gdmissionsystems.com/-/media/General-Dynamics/Cyber-and-Electronic-Warfare-Systems/PDF/Brochures/cyber-kiv-78-iff-crypto-datasheet.pdf?la=en&hash=104BCA305CDD5294A524F63F44374877BBB17537, accessed October 2018.

[5] GD MS. Personal communication with the IFF Engineering Project Leader, October 2018.

[6] Air Force Office of Scientific Research. "Mini Crypto chip is a Self-Contained Encryption Engine." Phys Org, https://phys.org/news/2017-10-mini-crypto-chip-self-contained-encryption.html, 4 October 2017.

[7] STTR/SBIR. "An Innovative NSA Authorized Design for a Micro IFF Transponder." https://www.sbir.gov/sbirsearch/detail/696115, 2014.

[8] IAI. "IAI Brings Light Weight IFF Technology to UAVs, Small Aircraft, and Dismounted Soldiers." https://www.i-a-i.com/2018/07/30/4291/, 30 July 2018.

[9] IAI. "MIFFT: Micro IFF Transponder." https://www.i-a-i.com/wp-content/uploads/2018/07/MIFFT_Brochure_04_25_2018_UPDATED-DISTRIBUTION-STATEMENT.pdf, 25 April 2018.

[10] SBIR/STTR. "Micro Identification Friend or Foe (IFF)." https://www.sbir.gov/sbirsearch/detail/696119, 2014.

[11] Raytheon. "KIV-77 Common IFF Applique Crypto Computer." https://www.raytheon.com/capabilities/products/kiv77, accessed October 2018.

[12] BAE Systems. "Identification Friend or Foe: KIV-6 Mark XII." https://www.baesystems.com/en/product/iff-family#iff_ccp, accessed October 2018.

[13] Thales Group. “IFF Crypto Components.” https://www.thalesgroup.com/en/iff-crypto-components, accessed October 2018.

[14] Hensoldt. “IFF Mode 4 / Mode 5 Crypto Computer QRTKxNG Family.” https://www.hensoldt.net/solutions/air/identification-iff/iff-mode-4mode-5-crypto-computer-qrtkxng-family/, accessed October 2018.

[15] Hensoldt. “QRTK3A/B NG: IFF Mode 4 / Mode 5 Crypto Unit for Transponders.” https://www.hensoldt.net/fileadmin/hensoldt/Solutions/Air/Surveillance_Reconnaissance/0415_17_QRTK3A_B_NG_datasheet_E_intranet.pdf, 2017..