Ensuring Secure Satellite Communications

Problem Statement

Satellite communications networks are indispensable assets for government and defence customers. One barrier to the adoption of commercial satellite capacity is concern over potential security risks. Specifically, that commercial satcom operators could access sensitive data or that third-party bad actors could compromise data once it leaves the satellite and moves over terrestrial networks. Addressing these concerns is critical to the adoption of commercial satcom services.

Arqit's Solution

Arqit offers an end-to-end encryption solution through SKA-Platform™, ensuring that data transmitted over Satcom—or in fact any telecommunications network—remains secure, inaccessible to operators or external actors. Symmetric encryption keys have long been used for defence and government and protect against current and future threats, including from a quantum computers, as they are not based on mathematical formulae that may be broken.

Key Features

1 **End-to-End Encryption:**
Encrypts data at every point, ensuring confidentiality from satellite to ground and across terrestrial networks.

2 **Over-the-Top Security:**
Adds encryption to voice and data traffic, maintaining security without relying on the underlying infrastructure.

Ability to change encryption keys frequently.

3 **Zero Trust & Quantum-Safe Encryption:**
Only authorised users can decrypt data, future-proofing against emerging cyber threats.

Proven Success with Satellite Networks

Arqit's solution has been successfully tested over satcom networks, including Inmarsat for drone communications and Eutelsat for secure VPN links. Verifying the platform's ability to secure data across satellite networks without impacting network performance.

Rigorous Security Validation

In the U.S., Arqit partnered with Juniper Networks, ensuring SKA-Platform meets National Security Agency (NSA) Commercial Solutions for Classified (CSfC) Symmetric Key Management Requirements. Independent Security Evaluators (ISE) analysis found no vulnerabilities, confirming the solution effectively mitigates man-in-the-middle attacks and ensures secure communications. SKA-Platform has been independently validated by **University of Surrey** and **PA Consulting**, strengthening confidence in its robustness.

Maintaining Sovereignty

To address concerns about sovereignty and data control, SKA-Platform can be deployed as an on-premise Private Instance. This ensures that the solution and data remains under full national control.

Proven Success and Integration

Arqit's solution is undergoing accreditation in key U.S. programs and is being integrated into offerings for the UK Ministry of Defence through UK primes. Additionally, the platform has been deployed by major companies in the Middle East, demonstrating its global applicability.

Conclusion

Arqit offers an over-the-top security solution with end-to-end encryption, ensuring that neither Satellite Operator nor any external actors can compromise sensitive data. By deploying the solution as a Private Instance organisations can maintain sovereignty and ensure secure communications.

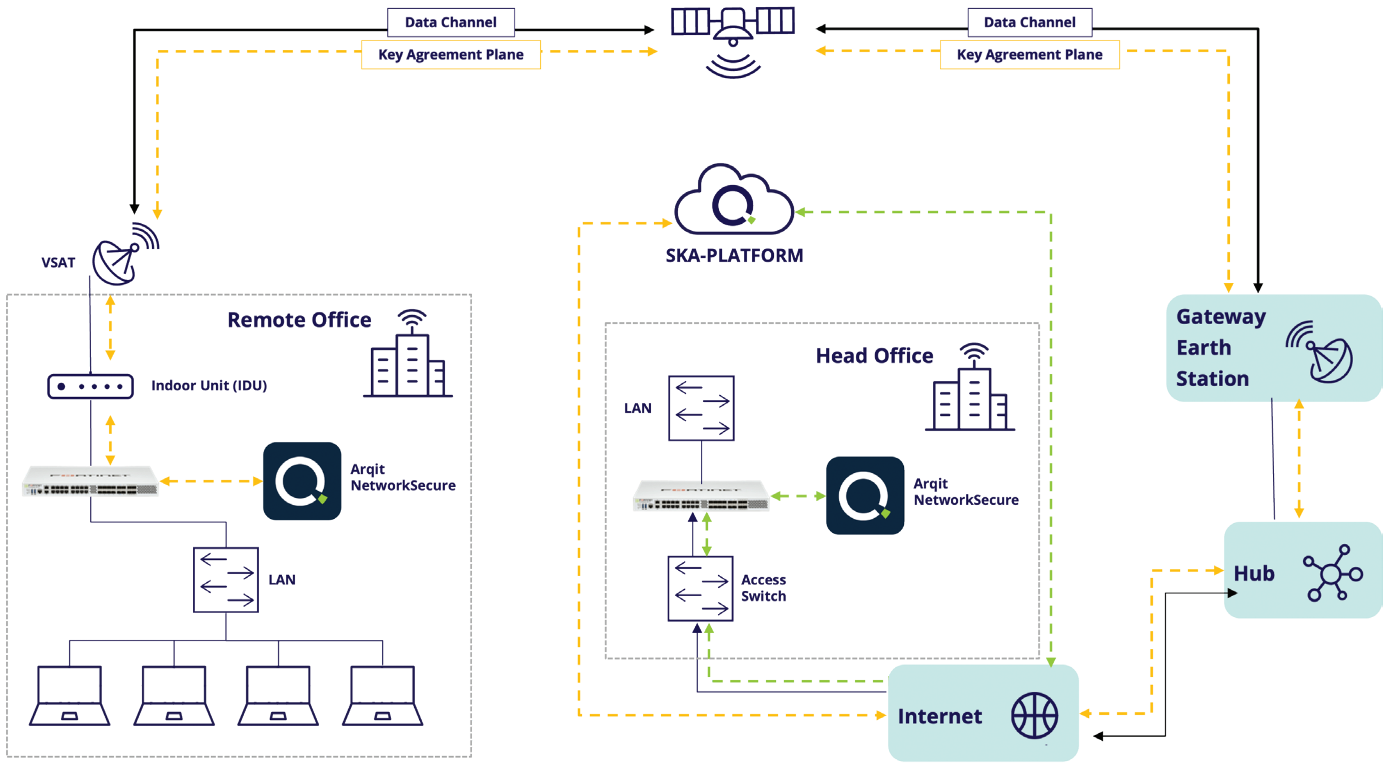

Figure 1: Deployment scenario for VSAT networks - provides end-to-end data security with symmetric encryption keys.

For more information, visit arqit.uk