STARLINK AND LEO SATELLITE NETWORK ENCRYPTION FOR GOVERNMENT AND DEFENSE:

Customer-controlled encryption for Government and Defense

The Low-Earth Orbit revolution

Orbiting 500–1,200 km above Earth, LEO constellations are rapidly transforming global communications. Securing these LEO satellite networks against interception and data compromise is now a critical requirement for government and defense organizations.

With thousands of satellites in dynamic mesh networks, providers such as Starlink, OneWeb, and Amazon LEO now deliver broadband connectivity with 30–50ms latency—comparable to terrestrial fibre.

LEO satellite capability is invaluable for:

Defense

Classified field communications

Mining

Secure OT data

Aviation

Secure air traffic control

Maritime

Encrypted vessel tracking

Humanitarian

Protect aid communications

With Low-Earth Orbit, your data crosses dozens of countries in minutes

Each jurisdiction is a potential interception point in the security of your data – end-to-end encryption with sovereign key control is the answer.

12,000 LEO satellites orbiting the globe in 2026.

500-1200 km altitude

2022 Viasat KA-SAT attack

Russia's invasion of Ukraine highlighted vulnerabilities in ground-segment systems, reinforcing that encryption without independent key control offers only partial protection.

From 'secure transport you must trust' to 'confidential transport you can control'

Satellite operators were once trusted by default, but modern zero-trust architectures assume no implicit carrier trust.

Comparison

Provider-Controlled Encryption	Customer-Controlled Encryption
Everything remains under the provider's management – cryptographic keys, algorithms, and firmware controls	You control all aspects of your own data – cryptographic keys, algorithms, and firmware governance
Decryption occurs inside provider-controlled ground infrastructure – reducing independent visibility into where and how data is processed	Data remains encrypted until it reaches customer-defined endpoints – maintaining a clearly defined cryptographic boundary
Key lifecycle management follows the provider's governance model – limited ability to define or audit cryptographic boundaries	Key lifecycle management is owned and auditable – full control over generation, rotation, and policy enforcement
Compliance alignment depends on the provider's controls and jurisdiction – sovereign key custody may not be independently verifiable	Supports alignment with FIPS 140-3, Common Criteria, and other sovereign requirements
Cryptographic upgrades and algorithm transitions follow the provider's roadmap and implementation timeline	Post-quantum and crypto-agile encryption – deployable on your own timeline, independent of the satellite provider's roadmap

Benefits of a cryptographic boundary

High assurance

Common Criteria EAL4+ & FIPS 140-3 Level 3 certification

Authenticated standards-based encryption (AES 256bit)

State-of-the-art encryption key management

Post Quantum Secure

Compliance and Obligation

ISO 27001

Don't just connect — connect securely. Senetas gives government and defense organizations sovereign encryption over any LEO satellite network.

Get the Starlink Encryption White Paper

Contact Us

Senetas
312 Kings Way
South Melbourne
VIC 3205 Australia

T: +61 (0)3 98684555
E: info@senetas.com

Senetas is an Australian defense technology company with 25+ years delivering certified network encryption to governments, militaries, and critical infrastructure operators across 60+ countries. Certified under Common Criteria, FIPS 140-3, US DoDIN APL, and NATO. Quantum-ready, NIST PQC-compliant, and delivered globally through strategic partner Thales.