GalacticQSL Lightpaper

Document Version: 1.0
Date: 10th March 2026
Classification: Public
Next Review: N/A

About This Lightpaper

This document is a lightpaper — a concise, accessible overview of a technology, product, or concept designed to give readers a clear top-level understanding without delving into deep technical implementation detail.

Lightpapers are intended for a broad audience, including technical and non-technical stakeholders, prospective partners, investors, and decision-makers who need to understand the strategic purpose, capabilities, and relevance of a solution. They sit between a marketing one-pager and a full technical white paper: substantive enough to convey real value, accessible enough to be read without specialist expertise.

For clients and partners requiring deeper technical documentation — including integration guides, API references, algorithm specifications, and compliance frameworks — Pan Galactic provides dedicated technical materials upon request and under appropriate confidentiality agreements.

Executive Summary

Modern digital infrastructure depends on cryptography. Every secure connection, identity system, and software supply chain relies on algorithms that protect data and verify trust.

However, advances in quantum computing are expected to render many widely used cryptographic algorithms vulnerable. Techniques such as RSA and elliptic curve cryptography could eventually be broken by sufficiently capable quantum computers.

Governments and standards bodies have therefore begun mandating a transition to **post-quantum cryptography (PQC)**to ensure long-term security.

GalacticQSL is Pan Galactic's **quantum-safe cryptographic library** designed to support this transition. It provides developers and organisations with a secure, standards-aligned foundation for building software systems that remain secure in the post-quantum era.

The library integrates both classical cryptographic algorithms and emerging PQC standards, enabling organisations to adopt **crypto-agility** while maintaining compatibility with existing infrastructure.

The Problem

Today's digital infrastructure was designed around cryptographic standards developed decades ago.

These include algorithms such as:

- RSA
- ECC
- ECDSA
- AES

While these algorithms remain secure against classical computers, they are expected to become vulnerable to **cryptanalysis using large-scale quantum computers**.

Two related security risks are already widely recognised:

1. **Harvest Now, Decrypt Later**
   Sensitive encrypted data intercepted today could be stored and decrypted once quantum capabilities mature.

2. **Harvest Now, Forge Later**
   Digital signatures and certificates could eventually be forged, allowing attackers to impersonate trusted systems.

This creates a strategic challenge for organisations operating critical infrastructure, particularly in:

- Space systems
- Defence communications
- Satellite command networks
- Secure data platforms
- Autonomous systems

Migration to post-quantum cryptography must begin years before quantum computers become capable of breaking current encryption.

The Pan Galactic Solution

GalacticQSL provides a **crypto-agile security library** designed to support both classical and post-quantum cryptographic algorithms within a unified framework.

Developers can use GalacticQSL as a foundational security layer for applications running across space systems, ground infrastructure, and secure data networks.

Key capabilities include:

- Support for classical cryptography for compatibility with existing systems
- Integration of emerging PQC standards for long-term resilience
- TLS 1.3 support for secure communications
- QRNG integration for high-entropy key generation
- Cryptographic primitives for encryption, hashing, digital signatures, and key exchange

The goal is to allow developers to transition gradually from classical cryptography to PQC without breaking interoperability or disrupting deployed systems.

How the Technology Works

GalacticQSL provides modular access to a wide range of cryptographic algorithms and primitives.

Classical Cryptography

These algorithms remain widely deployed and are necessary for compatibility with current infrastructure.

Examples include:

- RSA
- ECC
- ECDSA
- AES
- SHA-2 and SHA-3 hashing

These components ensure interoperability with existing TLS stacks, hardware devices, and software platforms.

Post-Quantum Cryptography

GalacticQSL integrates algorithms emerging from the NIST PQC standardisation process.

These include:

- Kyber (ML-KEM) for key exchange
- Dilithium (ML-DSA) for digital signatures
- SPHINCS+ hash-based signatures
- Falcon lattice-based signatures
- HQC code-based encryption

These algorithms are designed to resist attacks from quantum computers while maintaining performance suitable for real-world systems.

Future extensions will include support for advanced techniques such as **fully homomorphic encryption**, allowing computation on encrypted data.

Standards and Compliance Alignment

GalacticQSL is designed to align with internationally recognised security standards.

This includes:

- NIST PQC standardisation programme
- FIPS cryptographic module validation pathways
- ISO information security standards
- ECSS space system security guidance
- ETSI cryptographic and telecommunications standards
- 3GPP security frameworks
- UK NCSC guidance on quantum-safe cryptography

Pan Galactic intends to pursue **NIST cryptographic module validation** to ensure GalacticQSL can be adopted by organisations operating within defence and government procurement frameworks.

Deployment Environments and Use Cases

GalacticQSL can be embedded across multiple software environments.

Space systems

- Satellite command and control systems
- Secure satellite telemetry and communications
- Orbital data processing platforms

Defence and government infrastructure

- Secure communications systems
- Command and control networks
- Autonomous system security frameworks

Enterprise software

- Secure APIs and services
- Data encryption platforms
- Identity and certificate infrastructure

Why It Matters

Transitioning to post-quantum cryptography will be one of the largest security upgrades in the history of digital infrastructure.

Organisations that delay adoption risk exposing critical systems to long-term vulnerabilities.

Data and secure access credentials are being harvested now, largely without detection and this stolen data will be decrypted by those whom should not have access, this exposes a critical gap for sensitive data and creates a pathway for the potential take over of secure systems by threat actors.

GalacticQSL provides a practical pathway for organisations to begin adopting **quantum-safe cryptography today**, while maintaining compatibility with existing systems.

How It Fits Into the Pan Galactic Ecosystem

GalacticQSL forms the cryptographic foundation for the broader Pan Galactic platform.

It is integrated into:

- Galactic Secure Containers - our quantum secure containerisation solution
- GalacticOS - our plug and play quantum secure operating system
- GalacticQB - blockchain based network infrastructure

By embedding quantum-safe cryptography across the entire stack, Pan Galactic aims to provide a resilient digital infrastructure suitable for space systems, defence applications, and other critical environments.

Contact

For guidance on this document:
flow@pangalactic.io