KATIM

GATEWAY 9011

SECURITY FEATURES

THE BACKBONE OF ULTRA-SECURE COMMUNICATIONS

KATIM

GATEWAY 9011

KATIM Gateway 9011 has been designed to exceed the security requirements of the most demanding environments. State of the art hardware together with hardened software and hardened protocols enable protection of in-transit data with post-quantum cryptographic algorithms.

HARDENED PLATFORM

Hardware designed with security first mindset provides a trusted platform for software to run. An “always-on” dedicated Security MCU provides full device lifecycle tamper detection and response from factory to decommissioning. Persistently stored sensitive data is encrypted with a erasable key. In case tampering attempt is detected or emergency wipe of the device is requested, the master key is destroyed permanently and all sensitive data rendered inaccessible. In case the tamper event was found to be unintentional, a procedure is available to recover the device. Integrity protected security event log stores audit trail for full device lifetime.

Availability is an important property to consider for critical network infrastructure. KATIM Gateway is delivered under tamper control with redundant power supplies and fans that are tamper-protected yet field replaceable.

Even though KATIM Gateway 9011 has been designed to be deployed in physically secure locations, hardware implements risk mitigation for side channel leaks via EMI, power, sound or heat and various fault injection attacks. The H/W has been designed to meet FIPS 140-2 Level 4 criteria.

KEY BENEFITS

- A secure overlay solution using configurable crypto suite with post-quantum algorithms for securing data in transit.
- Next generation high performance hardware platform with full lifecycle tamper detection and response.
- Three-level physical red/crypto/ black isolation for reduced attack surface to sensitive data from external interfaces.
- Future-designed H/W with full S/W programmability to allow easy adaptation to future security needs.
- Custom-designed and hardened peer authentication, key exchange and tunneling protocol to mitigate several classes of vulnerabilities by protocol design.
- Best in market in-transit confidentiality and integrity protection via use of post-quantum algorithms, elliptic curves with 512-bit or stronger keys (equivalent to 15360-bit RSA), multi-seed RNG, authenticated encryption and narrow-scoped, short-lived keys.
- Application- and QoS-aware in-transit protection to minimise impact of traffic shaping in transit network.

CRYPTOGRAPHY

RANDOM NUMBERS

Generation of high quality random numbers is a key enabler for securing communications via cryptographic algorithms. Even a slight bias in random number generation could result in compromise of communications.

KATIM Gateway hardware is equipped with several independent non-deterministic hardware-based random number generators using internal components from multiple vendors. The entropy from the hardware-based generators is fed to the configured cryptographic suite's PRNG. This ensures highest possible RNG quality and ability to mitigate a compromise of individual hardware-based entropy sources.

CRYPTO SUITES

KATIM Gateway architecture supports crypto agility for integrating sovereign cryptographic algorithms. Due to flexible S/W and powerful H/W capabilities, most common cryptographic algorithms are suitable candidates for integration.

Once integrated, the algorithms are available for use in a crypto suite. The modular design of KATIM Gateway Tunneling Protocol allows configuring the crypto suite from pre-integrated set of algorithms. The configuration is locked for a S/W release to mitigate risks of negotiation attacks during session handshake.

According to latest research, traditional algorithms like RSA may be vulnerable to attacks made feasible by developments in quantum computing as factorisation of large numbers becomes more practical. The KATIM Gateway Tunneling Protocol leverages strong classical and modern post-quantum resistant algorithms to offer best-in-class protection against attacks made feasible quantum computers.

Phase	Purpose	Description
Handshake	Key Agreement	Authenticated classical key agreement with ephemeral keys combined with post-quantum algorithms
Handshake	Hash and Message Authentication	Multiple instances of 512-bit hashing and MAC algorithms
Handshake	Authenticated Encryption	Symmetric algorithm with 512-bit message authentication for 256-bit security
Payload Protection	Authenticated Encryption	Symmetric algorithm with up to 512-bit message authentication for 256-bit security

Table 1: Cryptographic algorithms overview

KEY MANAGEMENT

AUTONOMOUS KEY MANAGEMENT

A key benefit of the KATIM Gateway solution is autonomous key management with certificate-based authentication; manual pre-placement or rotation of encryption keys or shared secrets is not required. The autonomous key rotation mitigates risk of key leakage as manual operations with sensitive keys are not required and ensures short key lifetime for reduced window of opportunity for any malicious activity.

In the beginning of each handshake and re-handshake, a fresh set of unique, session-specific, random keys are generated. The re-handshake interval is customizable, and typically occurs every minute.

DUAL-LAYER KEY EXCHANGE AND AGREEMENT

Session handshake between KATIM Gateway's leverages multiple pairs of asymmetric keys. One set of keys is reserved for identity hiding during initial discovery handshake. A second pair of device unique asymmetric classical and post quantum keys with extreme key lengths protect the session handshake. A quad Diffie-Hellman procedure and triple KEM with post-quantum resistant algorithms are implemented in the handshake for further assurance. Ephemeral keys provide forward secrecy to mitigate against compromise of the static device-specific keys.

Independent keys are generated for protecting traffic in each direction for each QoS-aware encryption plane. Key material from NQ (non-quantum, classical) and PQ (post-quantum) handshakes are mixed and actual data protection keys are derived. During the re-handshake, all session-specific keys are completely re-negotiated.

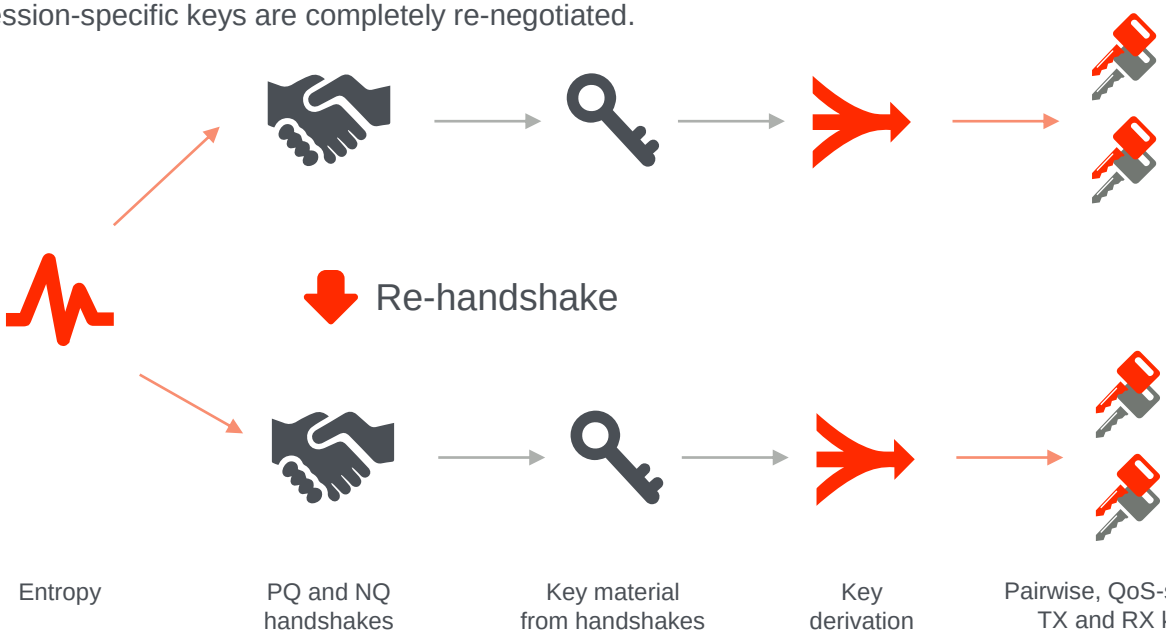


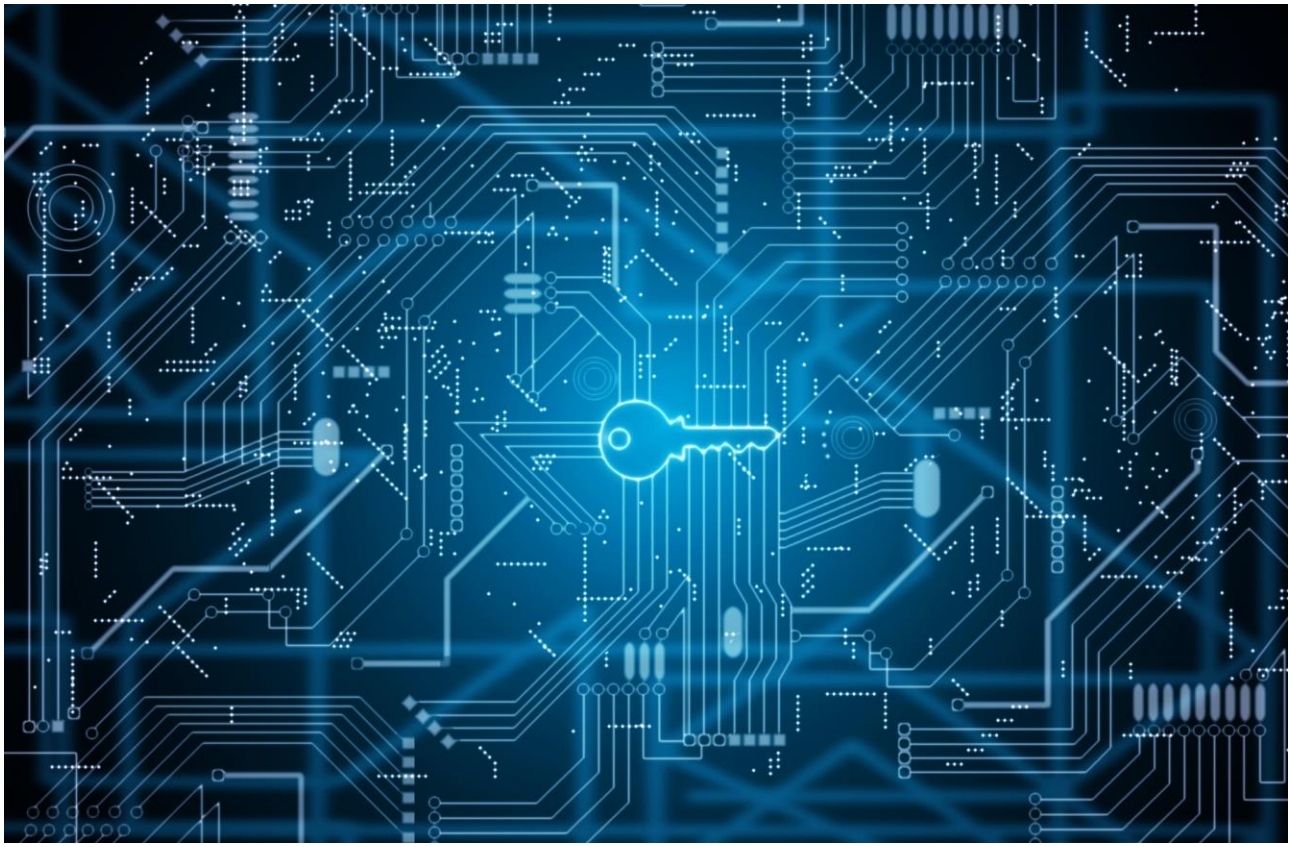
Diagram 1: Data protection key derivation and re-handshake flow

KEY LIFETIME

Autonomous key ratcheting enables frequent re-keying without control plane messaging. Once session has been established, the key ratcheting mechanism updates the data protection keys at frequent intervals. Key ratcheting happens autonomously by each peer independently by advancing the key sequence of TX and RX keys with a pre-determined algorithm. The key ratcheting interval is customisable and typically set to default of 131072 packets. Re-handshake and key ratcheting are conducted for each tunnel independently.

TUNNELED THROUGHPUT	AVERAGE PACKET SIZE	CALCULATED KEY LIFETIME
10 Gbps	9000 bytes	900 ms
10 Gbps	1500 bytes	150 ms
1 Gbps	1500 bytes	1500 ms
1 Gbps	353 bytes IMIX	370 ms
100 Mbps	353 bytes IMIX	3700 ms

Table 2: Examples of tunnel-specific calculated key lifetimes with specific bandwidth and packet size for key ratcheting interval of 131072 packets.



IN-TRANSIT DATA PROTECTION

MODERN APPROACH

Existing communication security protocols like IPSec or TLS have significant weaknesses which make them unsuitable for securing critical networks with high assurance requirements. Most of the existing protocols do not support post-quantum ciphers. Moreover, they are prone to classes of vulnerabilities that can be mitigated by keeping the protocol simple. As an example, many of SSL/TLS vulnerabilities are due to backwards compatibility (cipher downgrade attacks) or feature creep (Heartbleed).

Capability	Pure AES128/256	IPSec with IKEv2	TLS 1.2/1.3	KATIM Gateway Tunneling Protocol
Identity Hiding	N/A	✗	✗	✓
Post-Quantum Algorithm Support	✗	✗	✗	✓
Enforced re-authentication	✗	✗	✗	✓
Stealthiness	N/A	✗	✗	✓
Frequent Key Ratcheting	✗	✗	✗	✓
Simplified Handshake	N/A	✗	✗	✓

Table 3: Comparison of KATIM Gateway Tunneling Protocol with traditional protocols

CUSTOM TUNNELING PROTOCOL

KATIM Gateway Tunneling Protocol is based on a proven public cryptographic protocol design. The design has been amended with support for post-quantum algorithms for multi-layer handshake and reduced to mitigate classes of vulnerabilities by removing unnecessary features. The protocol design has been formally reviewed by an independent third party and has passed rigorous validation and review. Besides standard features like anti-replay and DoS protection, some of the key differentiators of the protocol are described in the following chapters in more detail.

DISCOVERY HANDSHAKE AND IDENTITY HIDING

Identity hiding in KATIM Gateway Tunneling Protocol is implemented with a discovery handshake. A deployment specific set of static discovery keys ensure confidentiality of the initial discovery handshake for exchanging device unique certificates. As device identities are not exposed in plaintext, a malicious actor observing the traffic is not able to identify the communicating parties. With TLS 1.2 or IKEv2 handshakes, the initial certificate exchanges may be observed by any party having access to the path between the gateways in transit network. In KATIM Gateway, this class of weaknesses is mitigated by protocol design.

ELLIPTIC CURVE KEY	EQUIVALENT RSA KEY	NOTES
160 bits	1024 bits	Widely used, not adequate anymore
224 bits	2048 bits	Widely used, should be phased out
256 bits (or 384 bits)	3072 bits (7680 bits, not feasible)	Current best practice for new deployments, not resistant to quantum computing attacks
512 bits	15360 bits	Used by KATIM Gateway

Table 4: Equivalent key lengths for classic (non-quantum) algorithms according to NIST SP 800-57 Rev 5 chapter 5.6.1.1

A solid foundation for data in-transit protection is provided by combination of well designed random number generation, classical algorithms, quantum computing resistant algorithms having extreme key lengths and short encryption key life-time.

DUAL LAYER HANDSHAKE

Control plane traffic in KATIM Gateway Tunneling Protocol is protected with dual layer handshake. Independent layers of classical and Post Quantum algorithms, both with extreme key lengths, ensure that compromise of single cryptographic mechanism will not compromise the control plane and key exchange. Cipher downgrade attacks have been mitigated by protocol and solution design.

APPLICATION-AWARE QoS HANDLING

To ensure availability of critical services and efficient use of bandwidth, KATIM Gateway allows mapping of traffic to fully independent application- and QoS-aware encryption planes. Each QoS-specific encryption plane uses separate encryption keys and any impact due to traffic shaping and policing in transit network is isolated to the affected encryption plane only. QoS marking for tunnels comprising the encryption plane and application to encryption plane mapping is fully user configurable. Firewalling on black and red ensures that only whitelisted traffic is accepted for further processing.

TIMERS AND COUNTERS

When session between KATIM Gateways has been established, continuous keepalive messages are exchanged separately for control plane and data plane for dead peer detection. Control plane keepalives and procedures enable fast dead peer detection while data plane keepalives ensure that data encryption keys stay synchronised. The most important timers and counters that drive these processes are described in the table below.

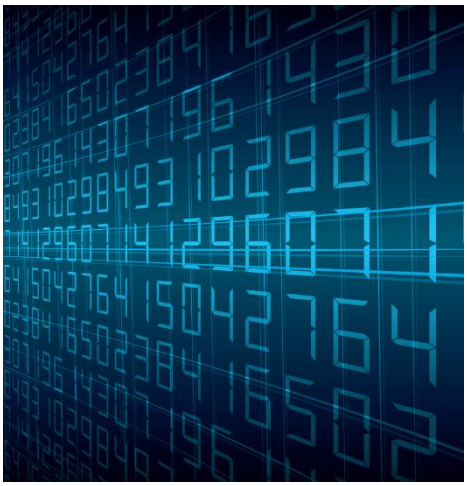
TIMER / COUNTER	PURPOSE
Discovery and handshake retry timer	Discovery and handshake is attempted at 10 s intervals.
Control and Data Plane Keepalive	The default values for control and data plane keepalives have been tuned for fast dead peer detection while ensuring that keys are synchronized across the peers.
Data Plane Key Ratchet Interval	Data Plane autonomous re-keying is enforced at configurable intervals and typically occurs every 131072 packets.
Re-handshake interval	Session between KATIM Gateways is re-established with full re-authentication and refresh of all data plane encryption keys and typically occurs once every minute.

Table 5: Timers and counters for KATIM Gateway Tunnelling Protocol

MANAGEMENT PLANE PROTECTION

ROLE-BASED ACCESS CONTROL

Segregation of duties is an important principle to consider in operational security design. KATIM Gateway enforces use of three administrative roles: Read-Only, Network Administrator and Security Administrator for daily operations while the fourth administrative role is reserved for initial customisation of the device. Each role is authorized for access to subset of device functionality and audit trail of every action is produced with personal accountability. For critical operations, like enabling packet bypass, un-tamper or tamper disarm procedures, two authorized administrators are required to enforce m of n access principle.



2-FACTOR AUTHENTICATION

Traditional username/password authentication is prone to credential sharing or theft. In event of such incident, it may take a while before the event is noticed and full impact is understood.

Each authentication token is prepared with an in-token generated private key. A certificate is issued that binds the private key to a identity with name and email address with a specific authorised role (Read-Only, Network Administrator, Security Administrator or Gateway Customisation).

REMOTE MANAGEMENT

Attack surface minimisation is an important key design principle for devices like KATIM Gateway that have been built to meet the most demanding security requirements. Only secure protocols with most secure ciphers are enabled for remote management. As an example, command line interface for remote management is available via SSH with strong ciphers and certificate-based authentication only. Similarly, SNMPv3 may be optionally enabled in authPriv mode only, or optionally protected with TLS, with the strongest standard ciphers supported for authentication (AES) and privacy (SHA).

SECURITY-CENTRIC APPROACH

One of the key design principles for KATIM Gateway development has been “defence in depth”. Single weakness or vulnerability in either hardware or software should not lead to compromise of the solution.

Industry standard best practices in product development like threat modelling, security risk assessment, architecture and design reviews, source code review, use of static analysis tools and dynamic security testing provide a solid foundation for secure product development.

As KATIM Gateway implements custom protocols, procedures and algorithms, security assurance plays a key part in product quality assurance. In addition to internal verification, independent 3rd party reviews have been conducted for critical subsystems of the solution: KATIM Gateway 9011 hardware, cryptographic functionality including random number generation, KATIM Gateway Tunnelling Protocol design and source code review of KATIM Gateway OS.

KATIM Gateway 9011 hardware has been designed to meet FIPS 140-2 Level 4 criteria.

All hardware and solution capabilities described in this white paper may not be supported in all software releases on all markets. Information is subject to change without notice.

Please contact KATIM representatives for further facts.

KATIM

KATIM is a leader in developing innovative secure communication products and solutions for governments and businesses. As an integral part of the Electronic Warfare & Cyber Technologies cluster at EDGE, one of the world's most distinguished advanced technology groups, KATIM stands as a beacon of trust in an ever-evolving landscape where cyber risks are a constant menace.

Our aim is to satisfy the growing demand for advanced cyber capabilities by delivering resilient, secure, end-to-end solutions across four fundamental business units: Networks, Ultra Secure Mobile Devices, Applications, and Satellite Communications.

With a global presence spanning from our headquarters in Abu Dhabi to offices in the UAE and Finland, KATIM empowers organisations worldwide with the unwavering assurance that their mission-critical information and communications remain private and secure, no matter the circumstance.

For more information, visit KATIM.com

KATIM

Peltokatu 26
Technopolis
33100 Tampere
Finland

KATIM

Elektroniikkatie 8
90590 Oulu
Finland

KATIM

Mikonkatu 9
Epicenter
00100 Helsinki
Finland

KATIM

Level 15, Aldar HQ
Abu Dhabi, United
Arab Emirates
+971 2 236 0600