BOScom
A SYSTEM MADE BY: WinIT GMBH

Willkommen in der Zukunft

BOScomQsEC_Quantum safe Enterprise Communication

Schütze deine Geheimnisse – vertraue deinem Netzwerk – einen Schritt voraus

DIE HEUTIGE VERSCHLÜSSELUNG IST VERALTET!

Mithilfe von Shors Algorithmus können Quantencomputer Daten entschlüsseln, die mit asymmetrischen Algorithmen (RSA, Elliptische Kurve) verschlüsselt wurden. Ihre Daten sind nicht mehr sicher. Wichtige, langfristig gespeicherte Daten werden bereits heute von Kriminellen gestohlen (harvesting), um sie morgen zu entschlüsseln (sogenannte „Steal-Now-Decrypt-Later"-Angriffe), sobald sie Zugriff auf kryptografisch geeignete Quantencomputer erhalten.

WARUM JETZT HANDELN ?

Das NIST veröffentlichte im August 2024 standardisierte Post-Quanten-Kryptographie-Algorithmen (PQC) und forderte die Industrie auf, „unverzüglich mit der Integration zu beginnen".

Warum ist es heute schon wichtig ?

- Investitionsschutz. Neu eingesetzte Assets müssen quantensicher sein!
- Vermeiden Sie Angriffe nach dem Muster „Erfassen, erst stehlen, dann entschlüsseln"!
- Die Umstellung auf quantensichere Algorithmen funktioniert sofort!

Warum BOScomQsEC ?

BOScomQsEC ist in der Lage, direkt in realen PQC-Implementierungen Schutz zu bieten:

- Sichere EDGE-zu-Cloud Anwendungen
- Sichere Mobile Devices und Netzwerke
- Sichere Satelliten Kommunikation
- Erfülle Defense C3 / C4

BOScomQsEC ist ein hocheffizientes, kryptoagiles Softwaremodul, das quantensichere öffentliche und private Schlüsselpaare mithilfe der quantensicheren kryptografischen Algorithmen des NIST generiert. BOScomQsEC kann außerdem quantensichere symmetrische Schlüssel für Standardanwendungen aushandeln und generieren.

Einfach zu implementieren – Einfach zu verwalten – Vollständig verwaltet oder unter Ihrer Kontrolle

Seien Sie Ihre erste Verteidigungslinie und sorgen Sie für Netzwerksicherheit !

BOScom
A SYSTEM MADE BY: WINIT GMBH

Willkommen in der Zukunft

Betriebsumgebung

Hybride Verschlüsselung
CISA, BSI und NIST befürworten „hybride" Post-Quanten-Kryptographie. BOScomQsEC kombiniert klassische Verschlüsselung mit der von NIST standardisierten Post-Quanten-Verschlüsselung.

Krypto-Agil
Das modulare Design von BOScomQsEC ermöglicht es dem Benutzer, kryptografische Algorithmen auszuwählen und im Betrieb umzuschalten.

Standards basiert
BOScomQsEC – Quantum saved Enterprise Communication kombiniert die heutigen bewährten Verschlüsselungsmethoden mit NIST-standardisierten quantensicheren Algorithmen.

Jetzt sofort Einsatzbereit
BOScomQsEC nutzt kernelbasierte symmetrische Verschlüsselung auf einer breiten Palette von Rechenoptionen, einschließlich EDGE-Gateways, Bare-Metal-Servern, VMs, Cloud- und Mobilgeräten, und ermöglicht so einheitliche Sicherheitsarchitekturen, die kritische Assets schützen, ohne dass ein kompletter Austausch erforderlich ist.

Topologien
BOScomQsEC ist eine softwarebasierte Kryptografietechnologie, die hochsichere Kanäle zwischen definierten Endpunkten herstellt, um Kommunikation und Datenübertragung vor heutigen und zukünftigen Quantenangriffen zu schützen. BOScomQsEC ist hardwareunabhängig, kann in neuen und bestehenden Systemen eingesetzt werden und ist mit einer Vielzahl von Rechenoptionen kompatibel. Die gängigsten Einsatztopologien sind:

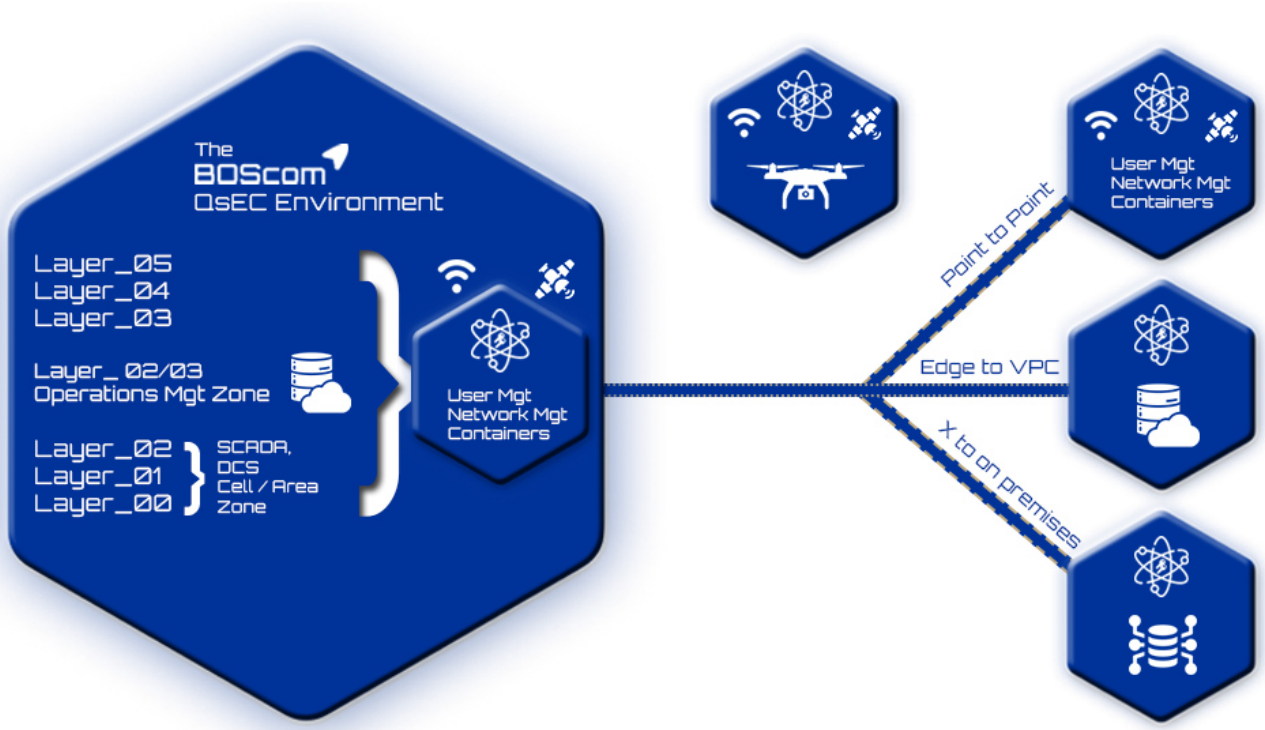
Point to Point
Eins-zu-eins-Kanäle zur Übertragung sensibler, vertraulicher oder personenbezogener Daten.
Beispiel: MPLS-Ersatz

Multipoint to Point (EDGE-to-Cloud)
Kommunikation von mehreren Assets und/oder Standorten zu einer virtuellen privaten Cloud oder einer privaten Cloud.

Multipoint to Point (on-premises)
Kommunikation zwischen verschiedenen Systemen und einem zentralen, lokalen Server.
Beispiel: Videoüberwachungskameras an einen Kameraserver

BOScom
A SYSTEM MADE BY: WinIT GMBH

Willkommen in der Zukunft



Spezifikation

Unterstützende Betriebssysteme

x86 based systems:
- RHEL 9
- Ubuntu 20.04
- Ubuntu 22.04
- Ubuntu 24.04
- Debian 11
- Debian 12
- Oracle Linux 9 UEK

ARM based systems:
- Ubuntu 22.04
- Ubuntu 24.04
- Raspbian OS
- Android 12+

RISC-V based systems:
- Ubuntu 22.04
- Ubuntu 24.04
- Debian 12

Leistung

- Latenz: < 1 msek
- Bandbreite: 99%
- CPU-Auslastung: < 5%

*Die tatsächliche Leistung kann in Ihrer Umgebung variieren und hängt von vielen Faktoren wie Durchsatz, MTU-Größe, CPU-Leistung usw. ab.

Wählbare Verschlüsselungen

- CRYSTALS-Kyber 1024
- CRYSTALS-Kyber 768
- Classic McEliece 460896
- Classic McEliece 4668828

Zukünftig werden weitere PQC-Algorithmen unterstützt.

Empfohlene Cloud-Endpunktkonfiguration

QsEC unterstützt cloudbasierte virtuelle Maschinen und Container:
- 2 GHz CPU, 4 cores
- 4 GB RAM
- 2 network interfaces

QsEC unterstützt standardmäßige virtuelle Schnittstellen von VMware, KVM und OpenStack. Die Anforderungen an CPU und Arbeitsspeicher hängen vom gewünschten Durchsatz und der gewünschten Latenz ab.

Empfohlene Edge-Endpunktkonfiguration

QsEC unterstützt ARM- und x86-Endpunkte:
- 1 GHz CPU
- 1 GB RAM
- 1 network interface

Unterstützte Netzwerktypen sind physische Ethernet-Schnittstellen einschließlich WLAN, 4G/5G und WinSAT*GOV....

QsEC schützt die Kommunikation, indem es internetseitige Netzwerkelemente verschleiert und eine hybride Post-Quanten-Verschlüsselung verwendet, um die heutige Verschlüsselung zu verbessern und nicht zu ersetzen !

Bitte senden Sie Ihre Anfrage per E-Mail an:
godigital@boscom.de

Wie empfohlen: WinSAT*GOV & BOScomQsEC ist Ihre beste Wahl !