FRAUNHOFER-INSTITUT FÜR PHOTONISCHE MIKROSYSTEME IPMS

PRESSEINFORMATION

Neues Key Management System (KMS) für die sichere Kommunikation der Zukunft

Fraunhofer IPMS entwickelt Key Management System (KMS) für quantensichere Netzwerke

Das Fraunhofer Institut für Photonische Mikrosysteme IPMS stellt ein neuartiges Key Management System (KMS) vor, das speziell für den Einsatz in quantensicheren Netzwerken entwickelt wurde. Dieses System verbessert den Austausch von geheimen Schlüsseln und sorgt dafür, dass Daten sicher über große Netzwerke verteilt werden können.

Traditionelle Methoden zur Schlüsselverteilung, wie RSA und Diffie-Hellman geraten angesichts der Rechenpower kommender Quantencomputer zunehmend unter Druck. Um diese Bedrohung zu umgehen und eine sichere digitale Kommunikation zu gewährleisten, nutzt die KMS-Software des Fraunhofer IPMS die Technologie der Quantenschlüsselverteilung (QKD), die auf der Basis von Quantenprinzipien beruht. Einzelne Punkt-zu-Punkt-Verbindungen lassen sich damit zu einem skalierbaren, sicheren Netzwerk verbinden, wodurch kryptografische Schlüssel symmetrisch und kontrolliert über mehrere Knoten und Domänen verteilt werden können. Das System schafft so eine zusätzliche, end-to-end-kontrollierte Sicherheits- und Kommunikationsschicht für besonders kritische Infrastrukturen. QKD ermöglicht nicht nur einen sicheren Schlüsselaustausch, sondern erkennt auch jegliche Abhörversuche und sorgt dafür, dass jede Störung sofort den beteiligten Parteien gemeldet wird. Die Einbindung von QKD in eine Cybersicherheitsstrategie bietet daher den bestmöglichen Schutz vor potenziellen Quantenbedrohungen.

Besonderheiten des Fraunhofer IPMS Key Management Systems (KMS)

Für Unternehmen, die auf quantensichere Kommunikation setzen, ist das Fraunhofer IPMS ein verlässlicher Partner. Mit langjähriger Expertise, innovativen Technologien und führender Forschung im Bereich Quantenschlüsselverteilung (QKD) unterstützt das Institut Unternehmen dabei, die Herausforderungen des Quantencomputings sicher zu meistern und zukunftsfähige Netzwerke aufzubauen. »Unser Key Management System ist das Herzstück komplexer QKD-Netze«, erklärt Dr. Alexander Noack vom Fraunhofer IPMS. »Es koordiniert Schlüsselanforderungen, erzeugt physikalisch gesicherte Schlüssel, verteilt sie zuverlässig und verwaltet ihren Lebenszyklus.« Die zentrale Steuerung über eine moderne, containerbasierte Architektur ermöglicht eine transparente, flexible und effiziente Verwaltung selbst großer Netzwerke. Dank ihrer hohen Skalierbarkeit lässt sich die Plattform sowohl in Forschungs- und Demonstrationsumgebungen als auch in großen Multi-Knoten-Netzwerken einsetzen.

Redaktion
Franka Balvin | Fraunhofer-Institut für Photonische Mikrosysteme IPMS | Telefon +49 351 8823-1144|
Maria-Reiche-Straße 2 | 01109 Dresden | www.ipms.fraunhofer.de | franka.balvin@ipms.fraunhofer.de

Mit dem ETSI GS QKD 014-konformen System setzt das Fraunhofer IPMS somit einen wichtigen Meilenstein für die sichere Kommunikation der Zukunft. Leistungsfähige Quanten-Zufallsquellen sorgen für höchste Sicherheitsstandards, während eine QKD-verschlüsselte Kommunikationsschicht den Schlüsselaustausch selbst über öffentliche Netze absichert.
Für die zukünftige Vernetzung mehrerer QKD-Domänen entwickelt das Fraunhofer IPMS derzeit eine Inter-Domain-Schnittstelle über Shared Trusted Nodes, die eine nahtlose Interoperabilität und Netzwerkerweiterung ermöglicht.

Anwendungsmöglichkeiten und Nutzen

Das KMS-System vom Fraunhofer IPMS befähigt Telekommunikations- und Metro-Netze, kritische Infrastrukturen wie Energie, Verkehr und Gesundheit, Rechenzentren und Cloud-Dienste sowie Behörden-, Forschungsnetze und Industrie-4.0-Umgebungen, eine Quantenschlüsselverteilung von Punkt-zu-Punkt-Verbindungen auf Netzwerkebene auszuweiten. So können Unternehmen oder Behörden mehrere Standorte gleichzeitig absichern, ohne für jede Verbindung eigene Punkt-zu-Punkt-Leitungen aufzubauen.
»Die Leistungsfähigkeit unseres Systems haben wir bereits im Projekt QuNET+MOBIXHAP erfolgreich unter Beweis gestellt, wobei verschiedene Szenarien von einfachen Labornetzwerken bis hin zu komplexen Topologien berücksichtigt wurden. Darüber hinaus ermöglicht unsere in Entwicklung befindliche Inter-Domain-Schnittstelle sichere Kommunikation über Domänengrenzen hinweg und schafft Investitionssicherheit für den ›Q-Day‹«, sagt Dr. Noack abschließend.

Detaillierte Informationen zu den Technologien der Quantenkommunikation am Fraunhofer IPMS sowie zum neuen Kommunikationsmanagementsystem stellt das Institut auf seiner Webseite bereit.

Über das Fraunhofer IPMS

Das Fraunhofer IPMS ist ein international führender Forschungs- und Entwicklungsdienstleister für elektronische und photonische Mikrosysteme in den Anwendungsfeldern Intelligente Industrielösungen, Medizintechnik und Gesundheit, Mobilität sowie Grüne und Nachhaltige Mikroelektronik. Forschungsschwerpunkte sind kundenspezifische miniaturisierte Sensoren und Aktoren, MEMS-Systeme, Mikrodisplays und integrierte Schaltungen sowie drahtlose und drahtgebundene Datenkommunikation. In den Reinräumen findet Forschung und Entwicklung auf 200 sowie 300 mm Wafern statt. Das Angebot reicht von der Beratung und Konzeption über die Prozessentwicklung bis hin zur Pilotserienfertigung.
Der Geschäftsbereich Data Communication und Computing (DCC) entwickelt als Experte für sichere Datenkommunikationslösungen innovative Technologien in den Zukunftsfeldern IP-Cores, Li-Fi (lichtbasierte Datenübertragung) und Quantum Technologies. Diese Entwicklungen ebnen den Weg für neuartige und sichere

Kommunikationslösungen in Schlüsselindustrien wie Mobilität, Telekommunikation, Industrieautomation oder der Energieversorgung.

Bildmaterial

Symbolbild für sichere Netzwerkkommunikation durch ein Key Management System ©AI generated

Dr. Alexander Noack, Gruppenleiter Data Communication & Computing am Fraunhofer IPMS
© Fraunhofer IPMS