KPN implementeert quantum versleutelde verbinding

Den Haag, 17 Mei 2016 - KPN heeft voor het eerst end-to-end quantum key distributie (QKD) toegepast in het netwerk tussen de datacentres van KPN in Den Haag en Rotterdam. Hierbij werkt KPN samen met ID Quantique, een Zwitsers bedrijf gespecialiseerd in quantum versleuteling. Hierdoor ontstaat een ongeëvenaard veiligheidsniveau voor het verzenden van vertrouwelijke informatie. KPN zal de komende jaren de mogelijkheden van quantum computing resistente versleuteling verder onderzoeken en ontwikkelen.

“Het verbeteren van de online veiligheid is topprioriteit voor KPN, niet alleen door het aanbieden van beveiligde netwerken en systemen, ook door te blijven innoveren met de laatste toepassingen en mogelijkheden uit de wetenschap waaronder quantum key distributie,” aldus Jaya Baloo, Chief Information Security Officer bij KPN. “De komst van de quantum computer over een paar jaar, maakt een groot deel van de bestaande encryptie methoden onveilig. De quantum computer is in staat rekenopdrachten die nu oneindig veel tijd vereisen, zoals een wiskundige aanval op een cryptografische algoritme, razendsnel op te lossen. Dit betekent dat bedrijven en organisaties nu al moeten gaan nadenken over nieuwe strategieën voor versleuteling, zoals QKD en ook hoe ze nieuwe post quantum cryptografie moeten toepassen.”

Quantum gedistribueerde informatie is niet te kopiëren en aftappen, afluisteraars of hackers zijn te detecteren. Door het inzetten van QKD in het netwerk wordt de versleutelapplicatie steeds van nieuw veilig sleutelmateriaal voorzien, die vervolgens gebruikt wordt voor gegevenscodering. Dit verhoogt de veiligheid van de versleuteling van gevoelige en vertrouwelijke informatie, waarmee klanten van KPN een ongeëvenaard veiligheidsniveau kunnen bereiken voor het verzenden van vertrouwelijke en gevoelige informatie.

Kelly Richdale, VP Quantum Safe Security bij ID Quantique zegt hierover: “Waar conventionele versleuteling is gebaseerd op wiskundige principes, is quantum versleuteling gebaseerd op natuurkundige principes. Dit geeft de mogelijkheid om informatie in het netwerk tussen verschillende datacenters te beschermen met een aantoonbaar hoog niveau van bescherming in de toekomst, zelfs na de komst van de quantum computer.”

Quantum versleuteling staat vandaag op de agenda tijdens Quantum Europe 2016, een conferentie over quantumtechnologie in het kader van het Nederlandse EU-voorzitterschap 2016. Kelly Richdale van ID Quantique zal daar ook spreken over quantum versleutelde verbindingen. Tijdens het evenement zal een “quantummanifest” worden gepresenteerd met een integrale strategie waarmee Europa met deze technologie tot de kopgroep kan blijven behoren.

Voor meer informatie:

Corporate Communications
Mediarelaties
Tel: (070) 446 63 00
Fax: (070) 446 63 10
E-mail: press@kpn.com

Investor Relations
Tel: (070) 446 09 86
E-mail: ir@kpn.com

KPN implement quantum encrypted connection (QKD)

The Hague, 17 May 2016 - KPN has implemented end-to-end quantum key distribution (QKD) in its network between KPN datacentres in The Hague and Rotterdam, the Netherlands. KPN is collaborating with ID Quantique, a Swiss company specialising in quantum encryption. KPN will use quantum key distribution to add an unmatched level of security for sending confidential information. In the coming years, KPN will further research and implement possibilities of post quantum encryption.

“Improving online safety is a top priority for KPN, not only by providing secure networks and systems for customers, also by continuously innovating with the latest advancements in science and technology including quantum," said Jaya Baloo, Chief Information Security Officer at KPN. "The arrival of quantum computers will ultimately render much of today's encryption unsafe. The quantum computer is capable of solving difficult mathematical problems exponentially quicker. Problems which would now take vast amounts of time, such as factoring attacks on encryption algorithms, would get a huge speed boost. This means that companies and organisations need to start thinking about new strategies for cryptography, such as increasing encryption key length, using QKD, and also developing and implementing post quantum cryptographic algorithms.”

Quantum information cannot be copied and eavesdroppers or hackers can be detected on the quantum link where the encryption key is exchanged. Quantum key distribution in the network enables the continuous generation and sharing of truly random keys which are then used for data encryption. This increases KPNs security and encryption of sensitive and confidential information, enabling customers to achieve unparalleled security for the transmission of confidential and sensitive information.

Kelly Richdale, VP Quantum Safe Security at ID Quantique said: "Where conventional cryptography is based on mathematical principles, quantum cryptography is based on quantum mechanical principles. This gives the ability to protect information across the network between data centres with a proven high level of assurance into the future, even after the advent of a quantum computer."

Today quantum encryption is also on the agenda during Quantum Europe 2016, a conference on quantum technology under the Dutch EU Presidency in 2016. During this conference, Kelly Richdale of ID Quantique will be talking about quantum key distribution. During the event a Manifesto will be presented containing a comprehensive strategy for Europe to stay at the forefront of this emerging technology.

About ID Quantique

ID Quantique (IDQ) is the world leader in quantum-safe crypto solutions, designed to protect data for the long-term future. The company provides quantum-safe network encryption, secure quantum key generation and quantum key distribution solutions and services to the financial industry, enterprises and government organisations globally.

IDQ also commercialises a quantum random number generator, which is the reference in the security and online gaming industries. Additionally, IDQ is a leading provider of optical instrumentation products, notably photon counters and related electronics.

www.idquantique.com