in Zusammenarbeit mit:

ADVA IDQ

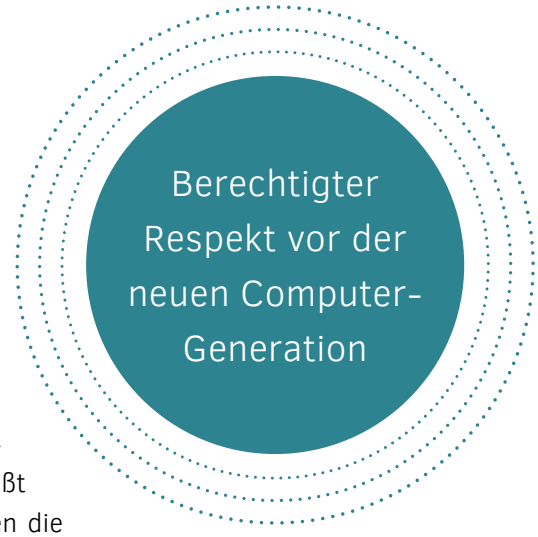
dacoso
data communication solutions

Lösungen für
langfristige Sicherheit

Herausforderung Quantum-Computing:
Auch in Zukunft sichere Daten

postquantumsafe

Quantum-Computing und die Folgen:
Das Ende der IT-Sicherheit?



Quantum-Computing – vor Jahren noch eine Vision, jetzt ungebremst anrückende Realität. Cloud Anbieter, IT-Entwickler und Geheimdienste arbeiten mit Hochdruck an einer neuen Generation von Computern. Keiner wird darum herumkommen, sich mit den Möglichkeiten, aber auch mit den Risiken auseinanderzusetzen. Berechtigterweise geht bei IT-Verantwortlichen die Sorge um: Was heißt das heute schon für die Sicherheit meiner kritischen Daten? Reichen die bisherigen Mechanismen noch aus, um sensible Unternehmensinformationen zuverlässig und langfristig vor Unbefugten zu schützen?

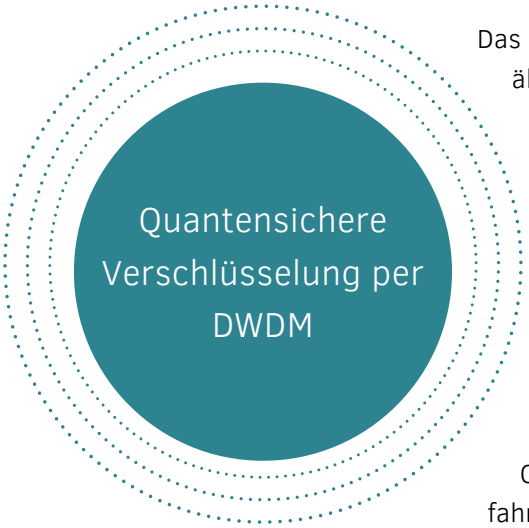
AES-256-Verschlüsselung hat weiterhin Bestand

Der Advanced Encryption Standard (AES) wurde 2001 offiziell standardisiert und ist heute der weltweit am weitesten verbreitete Verschlüsselungsalgorithmus. Dieser Erfolg gründet auf der leichten Handhabbarkeit und Sicherheit des Verfahrens – bis dato gibt es keine Anzeichen, dass AES-256 durch vollständige Schlüsselsuche erfolgreich angegriffen werden kann. Auch durch den Einsatz von Quantencomputern, die in Zukunft sehr wahrscheinlich die Leistung heutiger Supercomputer übertreffen können, wird sich die Schlüsselsuche nicht dramatisch verkürzen. Durch rasche Zyklen beim Wechseln der eingesetzten Schlüssel ist ein Angriff wenig lohnend; das Dechiffrieren selbst kurzer Sequenzen einer Nachricht ist immer mit dem vollen Aufwand der Schlüsselsuche verbunden.

Der Knackpunkt sind die Schlüssel-Austausch-Verfahren

Derzeit gängige Schlüsselaustauschverfahren wie Diffie-Hellmann ermöglichen, dass zwei Kommunikationspartner über eine öffentliche, abhörbare Leitung einen gemeinsamen geheimen Schlüssel in Form eines Informationsaustausches vereinbaren können. Die Schlüssel selbst sind nur diesen beiden Partnern bekannt und können nicht bzw. nur mit sehr viel Rechenleistung von einem potentiellen Lauscher berechnet werden. Das Verfahren basiert auf einem Algorithmus, dem eine mathematische Einwegfunktion zugrunde liegt. Das bedeutet, dass die Schlüsselgenerierung über eine sehr einfache mathematische Funktion erfolgt, für die Umkehrfunktion jedoch kein „schneller“ Algorithmus existiert. Allerdings sind heute schon Krypto-Analyseverfahren bekannt, die mit Hilfe von Quantencomputern erfolgreiche Angriffe auf derzeit verwendete Schlüsselaustauschverfahren möglich machen. Damit steigt das Risiko, dass heute übertragene, abgehörte und gespeicherte Daten zu einem späteren Zeitpunkt mit Quantencomputern entschlüsselt werden können.

Post-Quantum-Safe Key Algorithm:
Es wird neue beste Lösungen geben – und wir integrieren sie

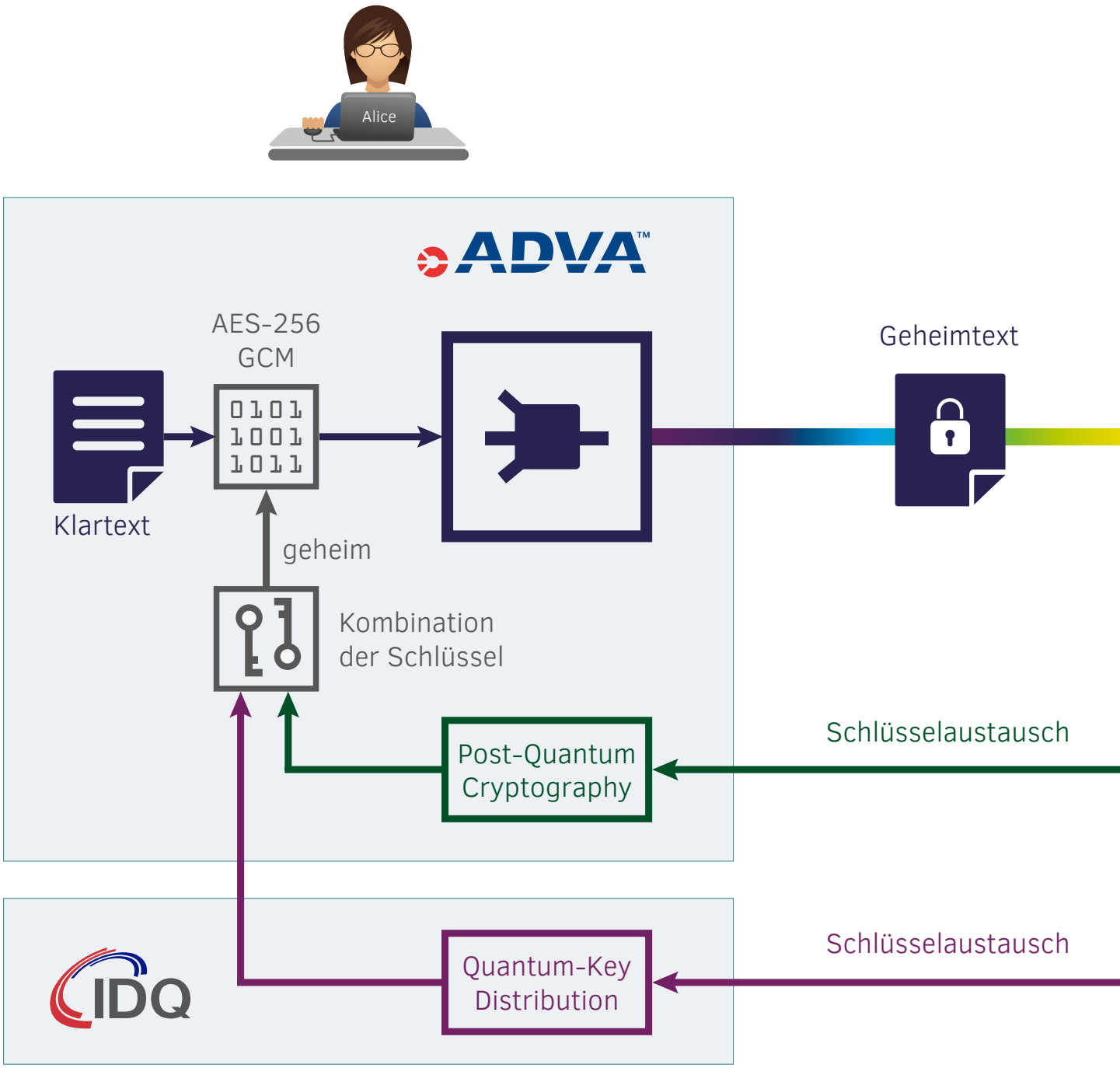


Das National Institute of Standards and Technology (NIST) ist eines der ältesten physikalisch-naturwissenschaftlichen Labors der USA und widmet sich allen Themen des Technology Leaderships. Weltweit hat es sich einen Namen als anerkanntes Gremium für Cyber Security gemacht. Das NIST analysiert die technologisch besten Lösungen für Schlüsselaustauschverfahren, die auch nach der Etablierung von Quantum Computing die Sicherheit bringen, auf die sich IT-Verantwortliche verlassen können.

Denkbar ist zum Beispiel ein Schlüsseltausch, der auf dem bis heute nicht geknackten McEliece/Niederreiter-Kryptosystem basiert. Oder es werden andere, neue Post-Quantum Computing (PQC)-Verfahren entwickelt und anerkannt: Die Lösungen, die sich als sicherste erweisen werden, hat ADVA künftig im Portfolio. Schon heute ermöglicht die ADVA-DWDM-Plattform mittels Software ein Upgrade der eingesetzten Schlüsselaustausch-Verfahren. Durch diese Flexibilität können die Systeme jederzeit auf den neuesten Stand der Krypto-Verfahren gebracht werden.

Quantum Key Distribution:
Abhörmanöver werden sofort entdeckt!

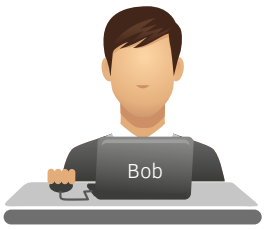
Die Schweizer Sicherheits-Spezialisten von ID-Quantique haben ein Verfahren auf Basis der Quantenmechanik entwickelt, mit dem eine absolut sichere Übertragung von Schlüsseln erfolgt. Jeder Versuch eines Abhörens durch einen Angreifer führt zum Verlust des Schlüssels (=Abbruch) sowie zum unmittelbaren Alarm. Das passiert auf der Glasfaserebene durch die Übertragungstechnik von ADVA mithilfe von QKD-Systemkomponenten an beiden Endpunkten. Dabei wird der Wert eines digitalen Bits auf einem einzelnen Quantenobjekt, einem QuBit, codiert. Das Abhören der zur Übertragung genutzten Glasfaser, z. B. mit einem Biegekoppler, führt zwangsläufig zu einer Störung, da dadurch Photonen verloren gehen. Ist also im Umkehrschluss die Übertragung des Schlüssels erfolgreich, ist der Nachweis erbracht, dass der übertragene Schlüssel nicht mitgelesen wurde und somit verwendet werden kann.



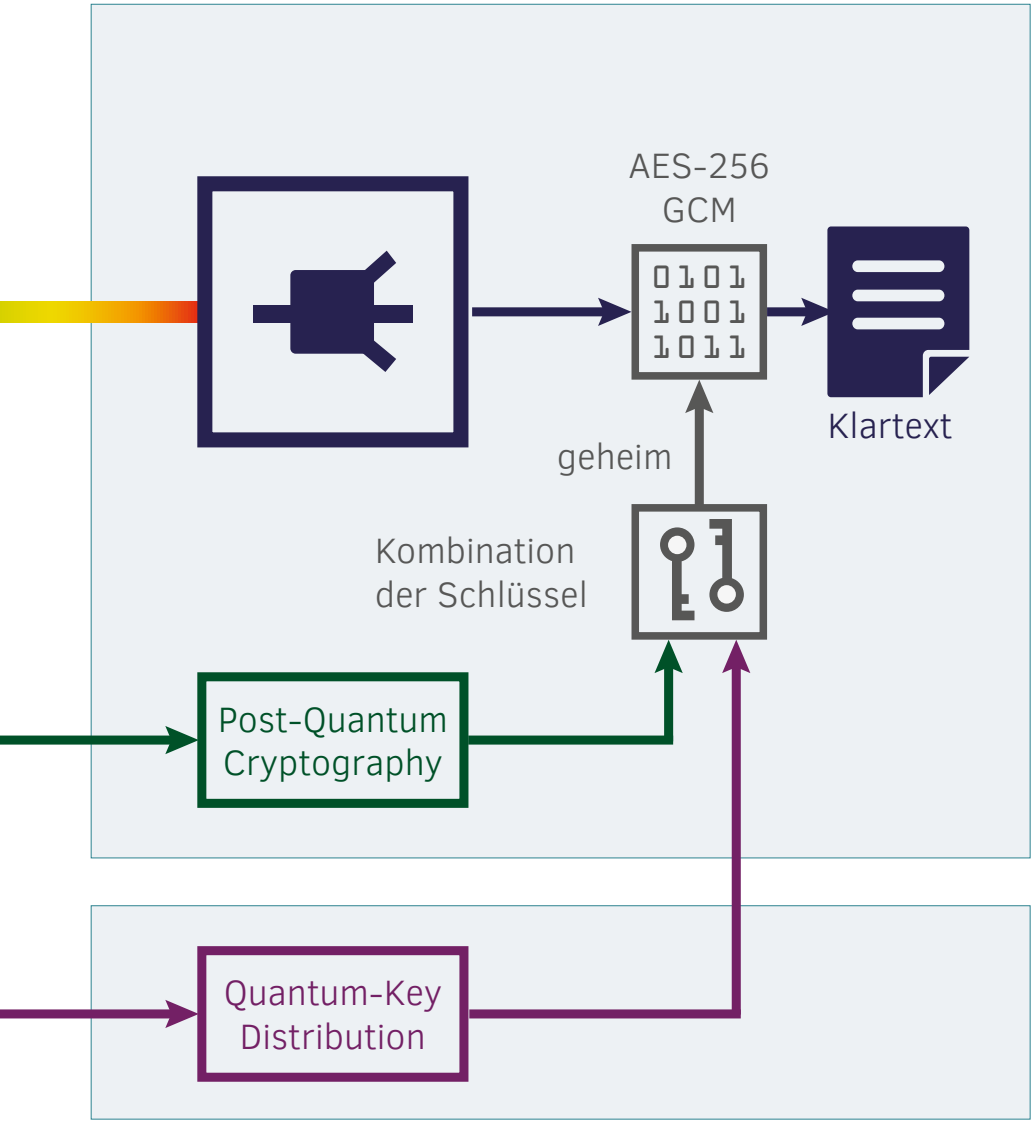
Wir machen das für Sie:

Expertise und Umsetzung aus einer Hand

dacoso ist ein Spezialist für Datenübertragung und die damit verbundenen Sicherheitsthemen und als Elite-Partner seit Jahren mit den DWDM- und Encryption-Lösungen von ADVA Optical Networking vertraut. Mit ID Quantique haben sich ADVA und dacoso einen neuen Partner ins Boot geholt, der das Konzept rund und vor allen Dingen maximal sicher macht: Durch die Kombination der bisherigen und neuen Verfahren für den Schlüsselaustausch erhalten Kunden zukunftsfeste Lösungen – für eine Sicherheit, die bei Marktreife und Einsatz von Quantencomputern erforderlich sein wird, um die Daten auch langfristig zuverlässig vor Bedrohungen zu schützen.



postquantumsafe



dacoso übernimmt auch für die neuen Verfahren alle Schritte von der Planung und Installation bis hin zur Inbetriebnahme und dem dauerhaften Betrieb. Mit dem sicherheitszertifizierten NOC/SOC (ISO 27001, BSI) erfüllt dacoso außerdem alle Anforderungen für eine Managed-Service-Lösung.

Installation,
Betrieb +
Überwachung

Über dacoso

dacoso bietet Lösungen für Connectivity, Cyber Defence und Virtual Networking. Als IT-Dienstleister richten wir uns damit an Unternehmen, die auf hochverfügbare und sichere Daten angewiesen sind und gleichzeitig agil bleiben wollen. Zu unseren Leistungen gehören unter anderem optische und nach BSI verschlüsselte Datenverbindungen, ein zertifiziertes Security Operation Center, Managed Security Services sowie Virtualisierungs-Lösungen, die für mehr Dynamik im Netzwerk sorgen.

Die dacoso GmbH ist ein inhabergeführtes Unternehmen mit Hauptsitz in Langen bei Frankfurt a.M. und 11 weiteren Standorten in Deutschland, Österreich und der Schweiz. Unter unseren Kunden sind Banken und Versicherungen, Unternehmen der Versorgungswirtschaft, Industrie und Handel, Einrichtungen der öffentlichen Hand sowie IT-Provider und Carrier. dacoso und seine Lösungen sind nach ISO 9001 und ISO 27001 zertifiziert.

Über ADVA Optical Networking

Innovation und der Ansporn, seine Kunden erfolgreich zu machen, bilden das Fundament von ADVA. Die Technologie liefert die Grundlage für eine digitale Zukunft und macht Kommunikationsnetze auf der ganzen Welt leistungsfähiger. ADVA entwickelt fortschrittliche Hardware- und Software-Lösungen, die richtungsweisend für die Branche sind und neue Geschäftsmöglichkeiten schaffen. Die offene Übertragungstechnik ermöglicht den ADVA- Kunden, die für die heutige Gesellschaft lebenswichtigen Cloud- und Mobilfunkdienste bereitzustellen und neue, innovative Dienste zu schaffen - für eine vernetzte und nachhaltige Zukunft. www.advaoptical.com

Über IDQ

ID Quantique (IDQ) ist der weltweit führende Anbieter von quantensicheren Kryptolösungen für den langfristigen Schutz von Daten. Das Unternehmen bietet quantensichere Netzwerkverschlüsselung, sichere Quantenschlüssel-Erzeugung und Quantenschlüssel-Verteilungslösungen für die Finanzindustrie, Unternehmen und Regierungsorganisationen weltweit. Außerdem vermarktet IDQ einen Quantenzufallszahlengenerator für die Spiel- und Sicherheitsbranche. Darüber hinaus ist IDQ ein führender Anbieter von optischen Messgeräten, insbesondere Photonenzählern und der dazugehörigen Elektronik. Die innovativen photonischen Lösungen des Unternehmens werden sowohl in kommerziellen als auch in Forschungsanwendungen eingesetzt. www.idquantique.com

dacoso
data communication solutions

dacoso GmbH
Deutschland | Robert-Bosch-Str. 25a | D-63225 Langen | T +49 6103 404 569 0
Schweiz | Riedstr. 1 | CH-8953 Dietikon | T +41 44 371 78 77
Österreich | Am Europlatz 2 | A-1120 Wien | T +43 1 717 28 324
info@dacoso.com | www.dacoso.com

BR-PQS-D-1909 | Fotos: Axel Boesten