# Agenda 22.03.2022 (Überblick)

## QuNET-Partnerworkshop #3

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

| 9:00 – 10:30 | PAUSE: 10:30 – 10:45 | 10:45 – 11:20 | 11:20 – 12:20 | PAUSE: 12:20 – 13:00 | 13:00 – 14:30 | PAUSE: 14:30 – 14:40 | 14:40 – 15:25 | PAUSE: 15:25 – 15:35 | 15:35 – 16:20 | PAUSE: 16:20 – 16:30 | 16:30 – 16:45 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Begrüßung / Vorstellungen / Einführung QuNETs | | Einführung in die Workshop Session / Fehlbedarfe + Pitches: QuNET+ML, QuNET+Reconnaitre | Pitches | | Komponenten & Hardware | | konzeptionelle & theoretische Arbeiten | | Software | | Auswertung der Sessions & Nächste Schritte |
| **Kontext** | | | **Networking** | | **Workshop / interaktiv** | | | | | | |

*inhaltlich analog zum 22.02.2022*

*Recap & Status nach dem 22.02.2022, + zus. Fehlbedarfe & Diskussionen*

Link: Plenum

# Agenda 22.03.2022 (Detail)

## QuNET-Partnerworkshop #3

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

| Von | Bis | Dauer | Thema | Sprecher |
|---|---|---|---|---|
| 09:00 | 09:10 | 00:10 | Begrüßung QuNET / Einordnung / Highlights | Schell |
| 09:10 | 09:20 | 00:10 | Vorstellung Institute + Teams | Mod. / LK |
| 09:20 | 10:00 | 00:40 | Vorstellung Teilnehmer | Alle |
| 10:00 | 10:10 | 00:10 | Ziele QuNET / Fokus QKD im behördl. Kontext / Ausblick | Mod. |
| 10:10 | 10:25 | 00:15 | Anwendungsszenarien, QuNET-Architektur, Schlüsselexperimente | Mod. |
| 10:25 | 10:30 | 00:05 | Bisherige Arbeiten & Ausblick | Mod. |
| 10:30 | 10:45 | 00:15 | PAUSE | |
| 10:45 | 10:50 | 00:05 | Einführung in die Workshop Session | Mod. |
| 10:50 | 11:00 | 00:10 | Fehlbedarfsübersicht: Aktueller Stand | Mod. |
| 11:00 | 11:20 | 00:20 | Pitches von QuNET+ML und QuNET+RECONNAITRE | Hock, Walter |
| 11:20 | 12:20 | 01:00 | Networking: Pitches (5 min., 2-3 Slides) | Alle |
| 12:20 | 13:00 | 00:40 | MITTAGSPAUSE | Mod. + Alle |
| 13:00 | 14:30 | 01:30 | Fehlbedarfe (1/3) zu Komponenten und Hardware | Mod. + Alle |
| 14:30 | 14:40 | 00:10 | PAUSE | Mod. + Alle |
| 14:40 | 15:25 | 00:45 | Fehlbedarfe (2/3) zu konzeptionellen & theoretischen Arbeiten | Mod. + Alle |
| 15:25 | 15:35 | 00:10 | PAUSE | Mod. + Alle |
| 15:35 | 16:20 | 00:45 | Fehlbedarfe (3/3) zu Software | Mod. + Alle |
| 16:20 | 16:30 | 00:10 | PAUSE | Mod. + Alle |
| 16:30 | 16:45 | 00:15 | Auswertung der Sessions + Nächste Schritte | Mod. |

Link: Plenum

# QuNET - Quantentechnologien für sichere Netze

Eine vom Bundesministerium für Bildung und Forschung geförderte Initiative der Fraunhofer-Gesellschaft, des Deutschen Zentrums für Luft- und Raumfahrt und der Max-Planck-Gesellschaft

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung


Fraunhofer

DLR

MAX PLANCK GESELLSCHAFT

Dritter QuNET-Partnerworkshop
am 22.03.2022

**Andreas Tünnermann**
Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF

**Martin Schell**
Fraunhofer Heinrich-Hertz-Institut HHI

**Christoph Günther**
Deutsches Zentrum für Luft- und Raumfahrt
Institut für Kommunikation und Navigation DLR-IKN

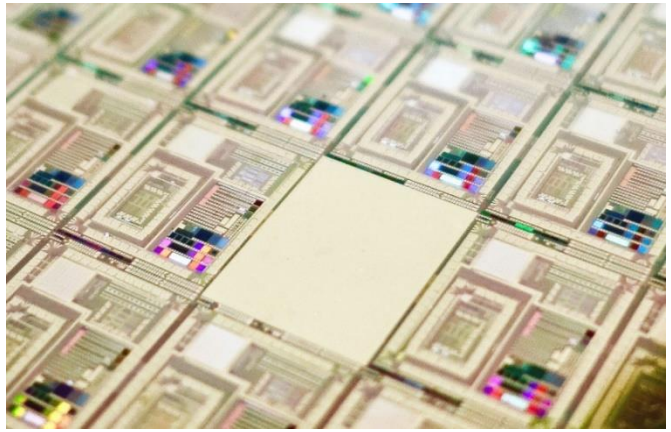
**Gerd Leuchs**
Max-Planck-Institut für die Physik des Lichts MPL

# QKD – Warum?

## Begegnung einer gesellschaftlichen Herausforderung

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Immer bessere Q-Algorithmen auf immer besseren Q-Computern bringen Q-Hacking einiger klassischer Verschlüsselungen in Reichweite.



MIT Technology Review

Computing

**How a quantum computer could break 2048-bit RSA encryption in 8 hours**

A new study shows that quantum technology will catch up with today's encryption standards much sooner than expected. That should worry anybody who needs to store data securely for 25 years or so.

by **Emerging Technology from the arXiv** May 30, 2019

Arbeitshypothese des BSI für den Hochsicherheitsbereich:

*"Anfang der 2030er Jahre gibt es mit einer signifikanten Wahrscheinlichkeit einen kryptografisch relevanten Quantencomputer"*

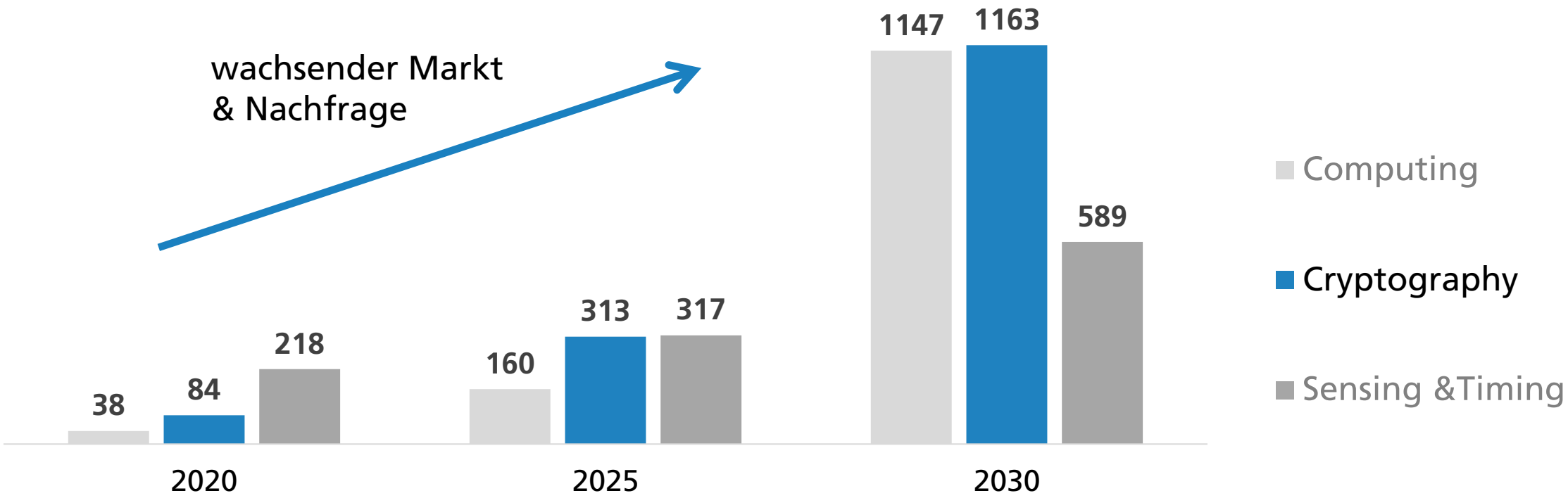
https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/

Siehe auch: Studie: Entwicklungsstand Quantencomputer, BSI, V1.1 (Juli 2019), https://www.bsi.bund.de/DE/Publikationen/Studien/Quantencomputer/quantencomputer_node.html

# QKD weltweit

## Marktentwicklungen (in Mio. $) in den Quantentechnologien

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

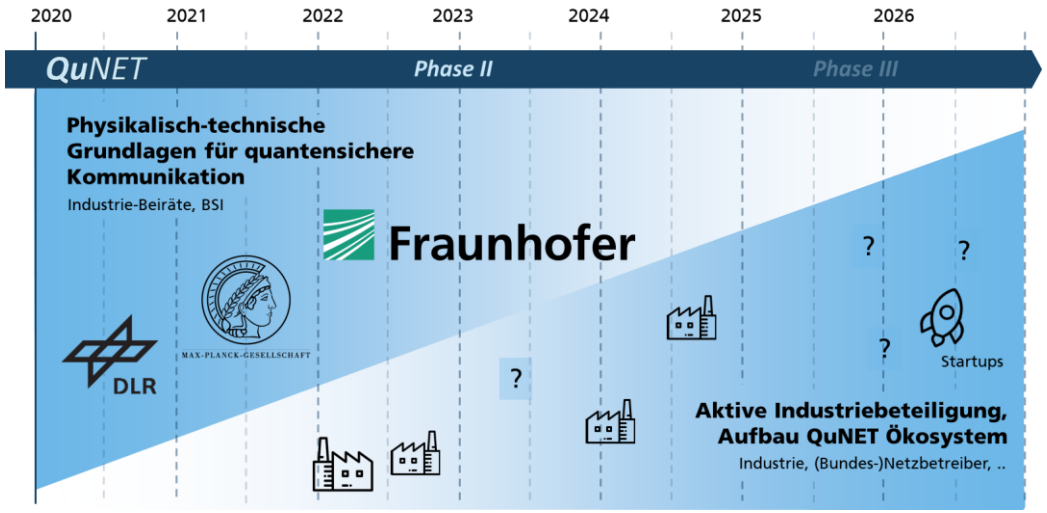



Quelle: Yole 2021

# QuNET - Überblick

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

- Nationale Initiative zur IT-Sicherheit zum Quantenschlüsselaustausch (**Quantum Key Distribution**, QKD), gefördert vom **BMBF**
- **Ziel**: QKD für hochsichere Kommunikation im behördlichen Kontext*
- Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (**BSI**), Kombination mit Postquantenverfahren (PQK)
- 7 Jahre Laufzeit (2019 - 2026), ca. 165 Mio € Projektvolumen
- **4 Kerninstitute + Beirat**
  - Max Planck Inst. Für die Physik des Lichts (MPL)
  - Deutsches Zentrum für Luft- & Raumfahrt (DLR-IKN)
  - Fraunhofer IOF
  - Fraunhofer HHI
- **[QuNET+]-Projekte** mit Industrie und Wissenschaft
- Transfer und wachsende Beteiligung der Industrie
- **Schlüsselexperimente**



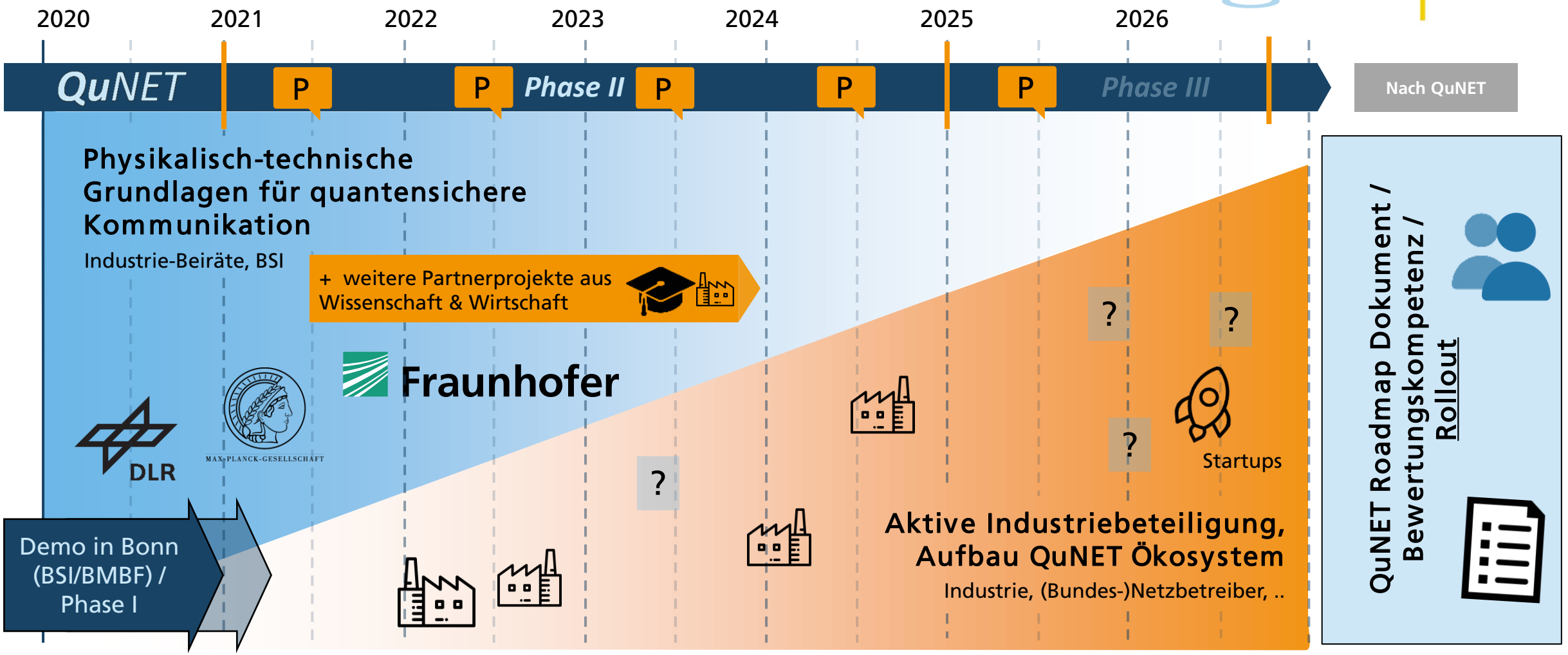

*oder Nutzern mit vergleichbar hohen Sicherheitsanforderungen in der Kommunikation. Homepage: https://www.qunet-initiative.de/




DLR
MAX-PLANCK-GESELLSCHAFT
Fraunhofer

# QuNET Initiative: Zeitschiene

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

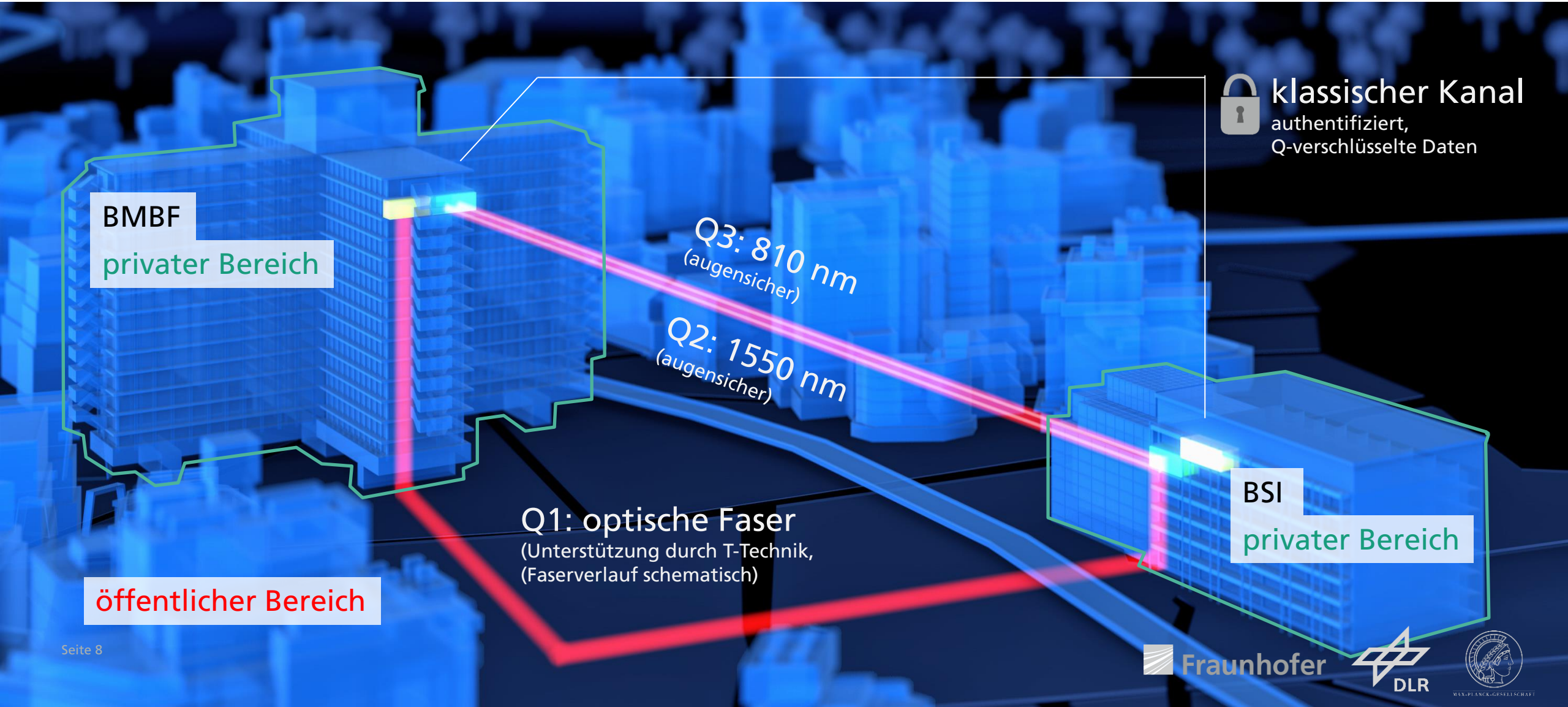


# QuNET Phase I / QuNET Bonner Demo

## Quantensichere Kommunikation: BMBF und BSI

QuNET

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung





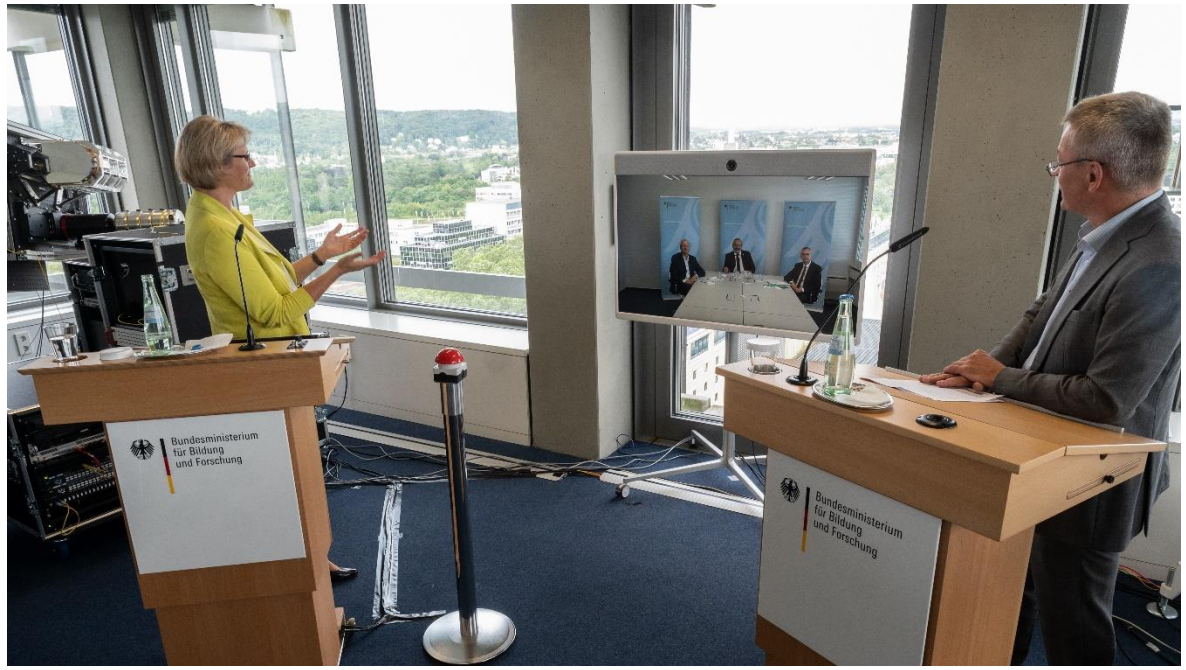

Fraunhofer DLR MAX-PLANCK-GESELLSCHAFT

# Bonner Demonstration

## (Konsortium) - Zusammenfassung der fachlich-wissenschaftlichen Ergebnisse

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

- QuNET befördert Akzeptanz & Sichtbarkeit der Technologie u.A. durch Schlüsselexperimente.
- Bonner Demo: Deutschland **erstmaliger Quanten-schlüsselaustausch zwischen zwei Bundesbehörden** und dessen Verwendung für eine sichere Videokonferenz
  - QKD-Systeme im Rackformat aus D, Aufbau durch Forscher vor Ort
  - Unterstützt vom BMBF (M, 513, Innerer Dienst., Projektträger, LS 21, uvwm)
  - Unterstützt vom BMI (CI / Könen, StS Richter)
  - Einbezug des BSI [KM 21, BL 34]
  - Technik kompatibel zu dt. Krypto-HW (R&S)
  - Unterstützung durch Deutsche Telekom Technik (Faser)
  - Unterstützung vom Beirat QuNETs (PK: Glingener)




https://www.bmbf.de/bmbf/shareddocs/pressemitteilungen/de/2021/08/100821-Quantenkommunikation.html

# Bonner Demonstration: Résumé und Ausblick

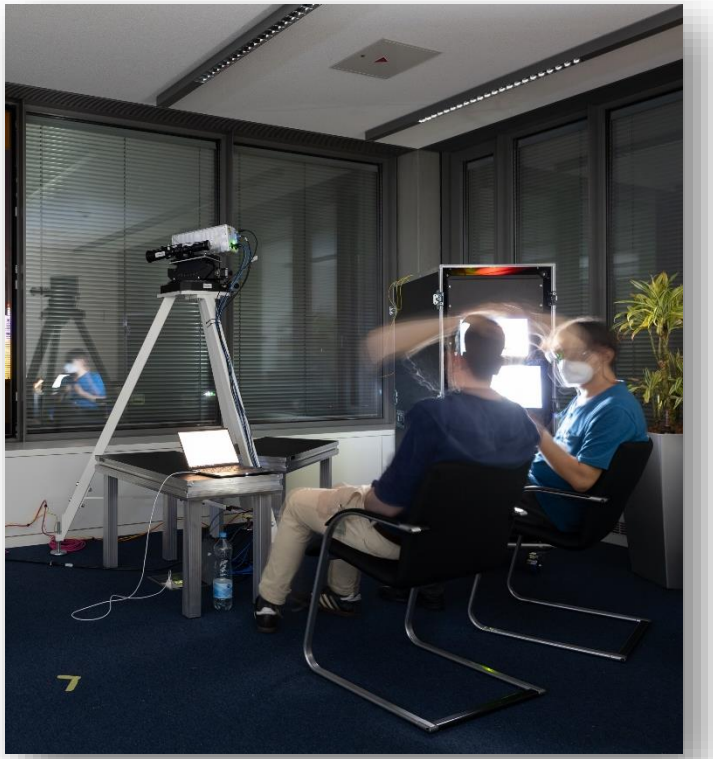
## (Konsortium / BMBF) - Impressionen

QuNET

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Bei Tag…



..und bei Nacht.





DLR

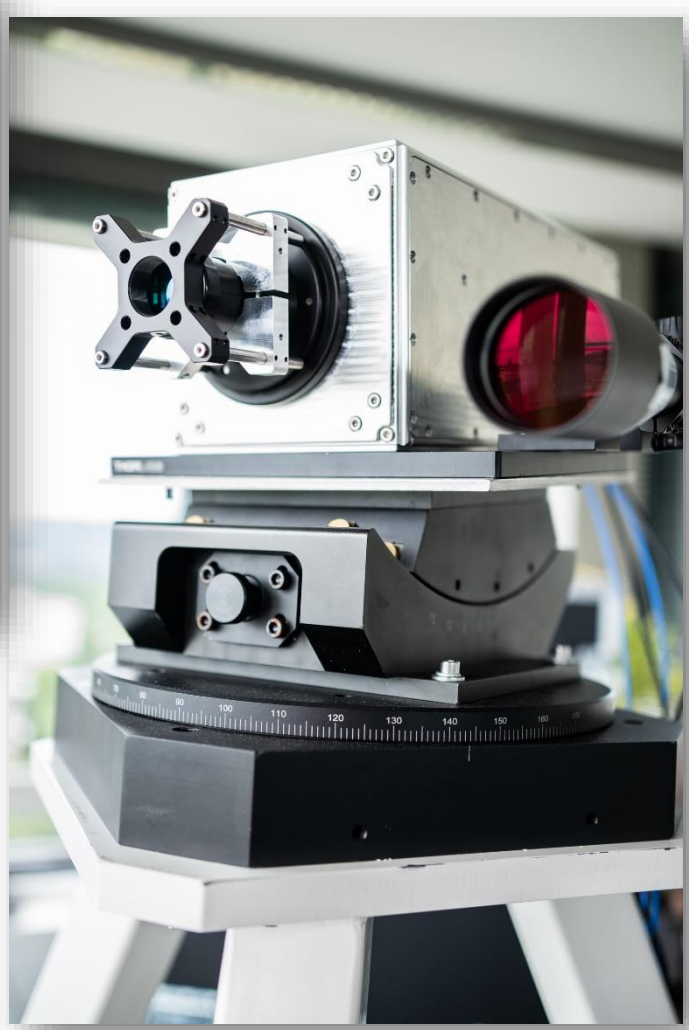
MAX-PLANCK-GESELLSCHAFT

Fraunhofer

# Bonner Demonstration: Résumé und Ausblick

## (Konsortium / BMBF) - Impressionen

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

# VORSTELLUNG DER INSTITUTE & TEAMS

durch je einen Vertreter des Instituts

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

# Vorstellung der Kerninstitute

## Komplementäre Kompetenzen

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

**Fraunhofer IOF**

*Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF*

**Q-Projekte**: QSource, QCtech, InteQuant, QPL, Applikations Labor Q-Engineering, Freistrahl-Testbed

**Kernkompetenzen**: Fasern, Freiformoptiken, Systemintegration, Mikro-&Nanostrukturierung uvm.

*Deutsches Zentrum für Luft- und Raumfahrt, Institut für Kommunikation und Navigation DLR-IKN*

DLR

**Q-Projekte**: QuNET, QUBE, BayernQSat, QUARTZ, SAGA

**Kernkompetenzen**: Global Connectivity, Global Positioning, Cyber Security, Autonomy and Cooperation, …

**Fraunhofer HHI**

*Fraunhofer-Institut für Nachrichtentechnik, Heinrich-Hertz-Institut HHI*

**Q-Projekte**: CiViQ, UniQorn, Q.Link.X

**Kernkompetenzen**: Photonische Komponenten, Netze & Systeme, Drahtlose Kommunikation, uvm.

*Max-Planck-Institut für die Physik des Lichts MPL*

MAX PLANCK GESELLSCHAFT

**Q-Projekte**: HQS, QUBE, QUARTZ, OpenQKD, BayernQSat, Super-Pixels, EuroQCI, ShoQC, CiViQ, ERC

**Kernkompetenzen**: Theorie, Nano-Optik, Optik & Information, photonische Kristallfasern uvm.




DLR
MAX-PLANCK-GESELLSCHAFT
Fraunhofer

# Vorstellung der Gäste

## Inkl. BMBF, Beiräte, Gäste.

Stand 22.02.:
30 min vorgesehen

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Bitte stellen Sie in ca. <1 Minute **sich selbst** & ihr **Unternehmen/Affiliierung** vor, und was ihre **Motivation** ist sich in sicherer Kommunikation zu engagieren?

| WS #2 | WS #3 | 22.02 & 22.03. | Affiliation |
|---|---|---|---|
| 23 | 16 | 35 | Industrie |
| 7 | 7 | 11 | Akademia |
| 6 | 21 | 19 | AUFs |
| 4 | 1 | 4 | Sonstige |
| 17 | 0 | 17 | QuNET |
| 1 | 0 | 1 | unbekannt |
| 58 | 45 | 87 | Summe |

| Beiräte | Affiliation |
|---|---|
| Andreas Gladisch | Deutsche Telekom / T-labs |
| Christoph Glingener* | ADVA Optical Networking |
| Stefan Kück | PTB |
| Patrick Leisching | TOPTICA Photonics AG |
| Manfred Lochter | BSI |
| Peter van Loock | Uni Mainz / Q.Link.X |
| Klaus Michel | TESAT-Spacecom |
| Stefan Röhrich | Rohde & Schwarz Cyber Security |
| Bernhard Sang | OHB |
| Michael Waidner | National Digital Hub Cyber Security |
| Henning Weier | Qutools / Quantum Space Systems |
| Felix Wissel | Deutsche Telekom / Technik |




→ Vorstellungen: (nächster Slide)

# ZIELE QUNETS

Ziele, Fokus QKD in realistischen Anwendungsszenarien

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

# Ziele

## Schlüsselverteilung für zukünftige quantensichere Kommunikation

QuNET

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung




Fraunhofer DLR MAX-PLANCK-GESELLSCHAFT

# Ziele

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

- Die Ziele QuNETs liegen in der Befähigung der für die IT-Sicherheit in behördlicher Kommunikation relevanten Anwendungsszenarien und den dafür benötigten QKD-Systemen für die quantensichere Kommunikation
  - Ziel 1. Zwischen zwei Zugangspunkten in jeweils einem Hochsicherheitsbereich
  - Ziel 2. Mehrere Zugangspunkte in jeweils einem Hochsicherheitsbereich
  - Ziel 3. QKD für große Multi-user Netze und Verknüpfung von mehreren Netzwerken

- Die Anwendungsszenarien werden in verschiedenen Schlüsselexperimenten (SE1 – SE4) adressiert. Die SE setzen dabei Teilaspekte der QuNET-Architektur als temporäre QuNET-Pilotnetze um.

# QuNET – Anwendungsszenarien

## Befähigung von QKD in real. Szenarien insbes. im behördlichen Kontext

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

SE1

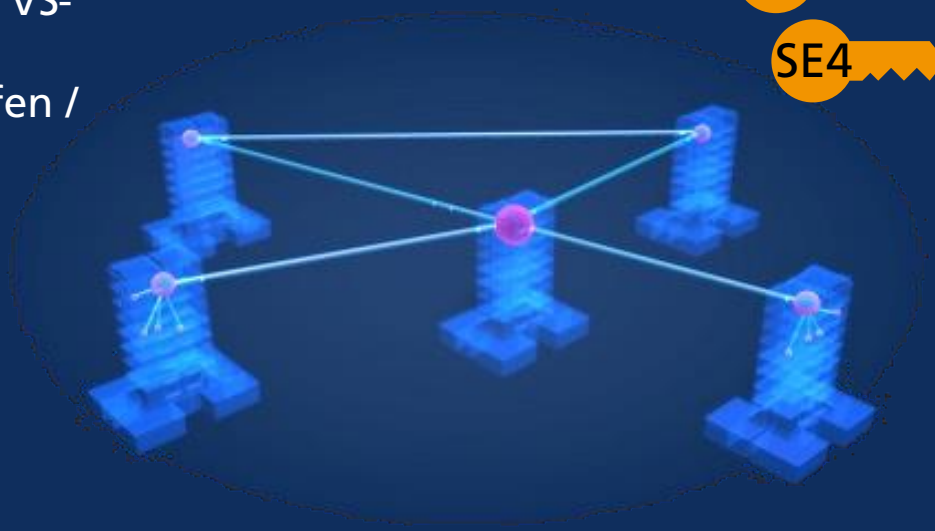
SE2

### Anwendungsszenario I (p2p)

Kommunikation (insbes. betreffend Daten mit langen Geheimhaltungsfristen) zwischen einzelnen Behörden (z.B. VS-Dok-Speicher), ausgewählte Viko-Leitungen, Botschaften, Gipfeltreffen / ad-hoc

### Anwendungsszenario II (mehrere Zugangspunkte)

Behördennetze (mehr als 2 Behörden)



SE3

SE4

### Anwendungsszenario III (weitverzweigte Netze, End-Nutzer zu End-Nutzer)

einzelne Mitarbeiter/Arbeitsgruppen innerhalb einer Behörde

### Anwendungsszenario IV

Beyond QKD / Querschnittsszenario



Fraunhofer DLR MAX-PLANCK-GESELLSCHAFT

# Quantenphysik & Quantenkryptografie

## Zukünftig zwei komplementäre Lösungen

QuNET

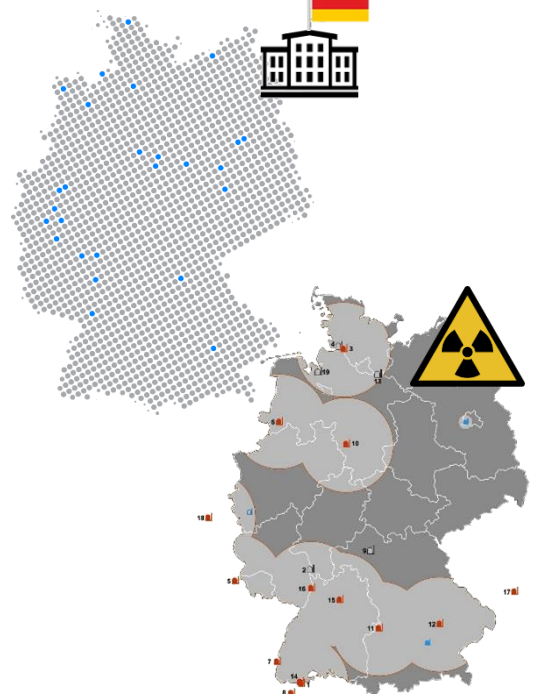
GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

### Post-Quanten Kryptografie (PQK)

- Resilienz gegen *bekannte* Q-Computer Algorithmen & Leistung
  - Arbeitsplatzrechner, mobile electronics, ..
- Einfachere Implementierung (€)
- Komplementär zu QKD, z.B. via KDF (Schlüsselkombination)

### Quantum Key Distribution (QKD)

- Erfüllt (komb. mit PQK) extreme Anforderungen an Sicherheit*
  - Kritische Infrastruktur
  - Banken
  - Versicherungen
  - Regierungen (NdB)
- Höhere Schlüsselraten (€)
- Zukunftssicher, auch gegen Speicherangriffe







Standort-Karten: 1) Oberste Bundesbehörden + 61 Bundesoberbehörden (Aufsichtsbehörden) + 28 Bundesanstalten + 3 Körperschaften des öffentlichen Rechts; 2) Standorte dt. Atomkraftwerke

*bis zur Messung/Entschlüsselung. Danach sind andere klassische IT-Sicherheitsmaßnahmen erforderlich.

DLR
MAX-PLANCK-GESELLSCHAFT
Fraunhofer

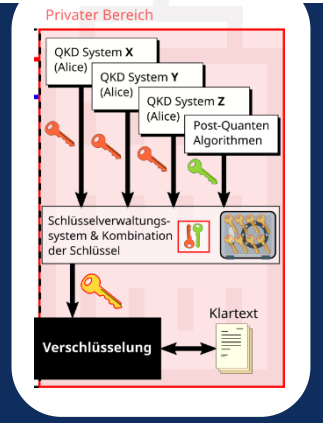
# QuNET – Arbeiten der Kerninstitute

## Konzepte, Technologien und Komponenten

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

**AP1**: Systemkonzept eines Gesamt-netzes (Christoph Marquardt, MPL)

- QKD in der IT-Sicherheit (ganzheitlicher Ansatz)
- sichere, praktische, skalierbare und kompatible Systemarchitekturen



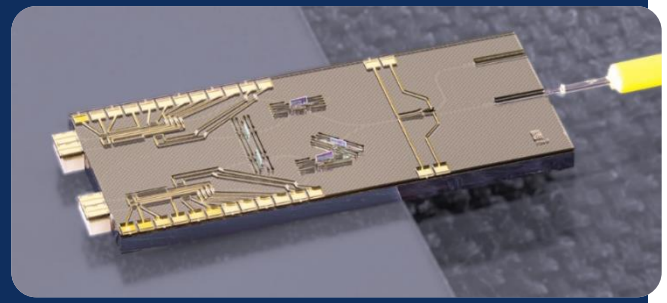

**AP3**: Überwindung technischer Einschränkungen (Florian Moll, DLR)

- Kanal und Netztechnologie (Faser, FS
- Weite Distanzen, Anbindung Q-bits
- Konversion von Q-Zuständen,

**AP0**: Koordination / Wissenschaftskommunikation (QuNET-Office, Markus Selmke, IOF)

**AP2**: Bausteine zur techn. Souv. in Q-sicheren Systemen (Fabian Steinlechner, IOF)

- Feldtaugliche (z.T. integrierte) Sender- und Empfängerkomponenten
- Komponenten für Backbones
- Systemkomponenten



**AP4**: Zertifizierbare QKD-Gesamtsysteme (Nino Walenta, HHI)

- Implementierung von CV-, DV, und verschränkungsbasierten QKD-Gesamtsystemen
- Berücksichtigung nationaler Zertifizierungsanforderungen

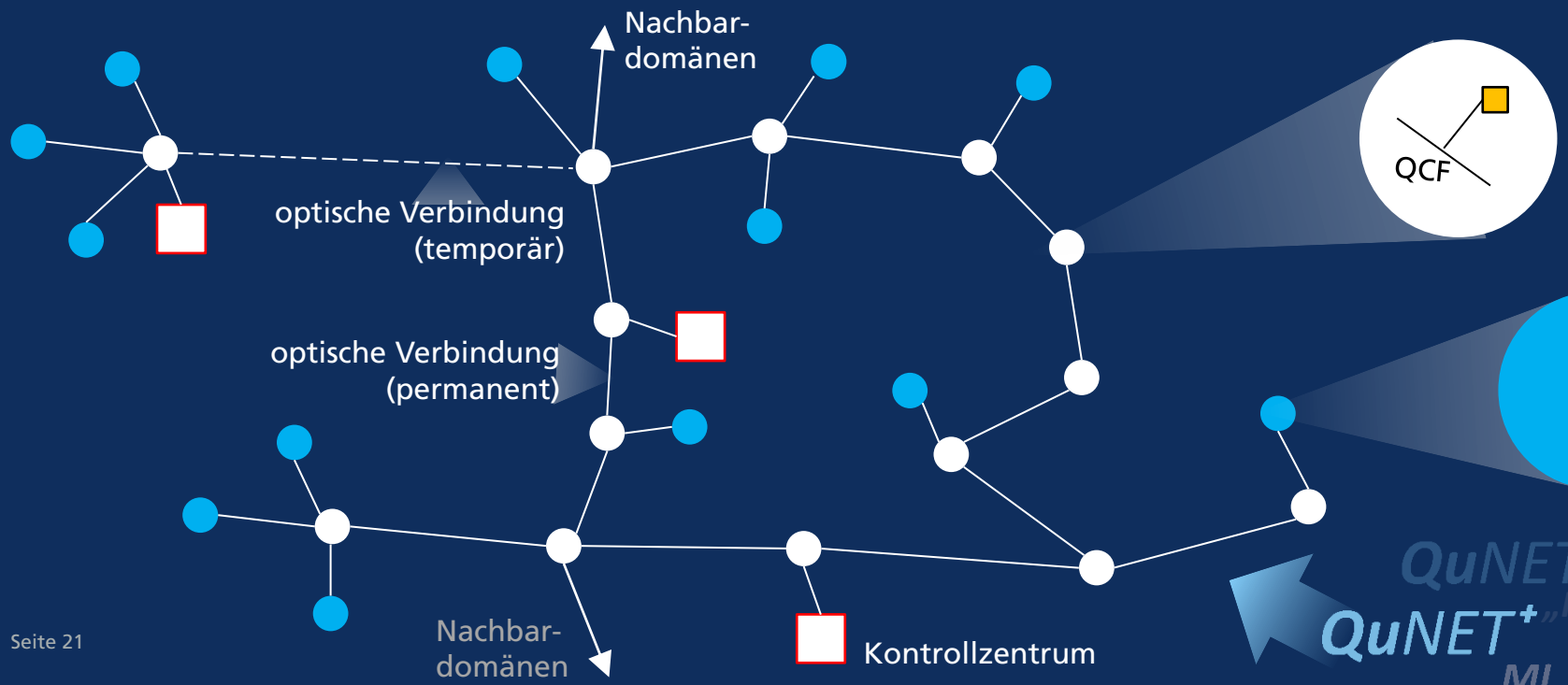
# QuNET – Architektur [AP1]

## Interoperable und integrierbare Architektur zur Nutzung von QKD (Stand Q1-2022)

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

- QKD: Ende-zu-Ende Sicherheit wo möglich
- Einbezug von Post-Quanten-Kryptografie
- Upgradefähig: Quanten-Repeater, Satellit, EuroQCI
- Optisches Routing / Switching / (R)OADMs / LWL-Panels / SDN

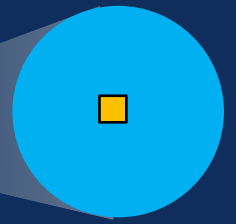
- BSI-Richtlinien
- Weitestgehend QKD-Protokollagnostisch
- (+ klassisches Kommunikationsnetz / IT-Sicherheitsinfrastruktur)







**Zwischenknoten** nutzen Quanten-klassisch-(QC)-Filter, ggf. Q-Repeater, Switch oder Schlüssel per QKD-Modul



**Endknoten** beinhaltet QKD-Modul. Modular, standardisierte Schnittstellen (e.g. an Verschlüssler)

QuNET+
„KMS“ (tbd)
QuNET+
ML



Fraunhofer DLR MAX-PLANCK-GESELLSCHAFT

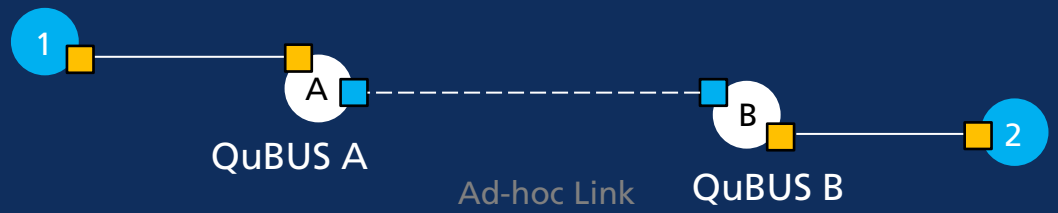
# QuNET – Schlüsselexperimente [AP5-8]

## Demonstration von Funktionalitäten der QuNET-Architektur

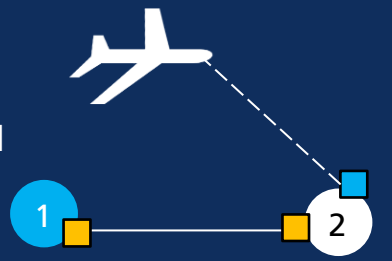
GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

- **Schlüsselexperimente** erbringen neue Funktionsnachweise sowie Funktionalitätserweiterungen für behördliche Hochsicherheitskommunikationsanwendungen.
  → SE setzen **Teilaspekte der QuNET-Architektur** als temporäre **QuNET-Pilotnetze** um.

### SE1 (Ende 2022)




### SE3 (Anfang 2025)




QuNET+ RECONNAITRE

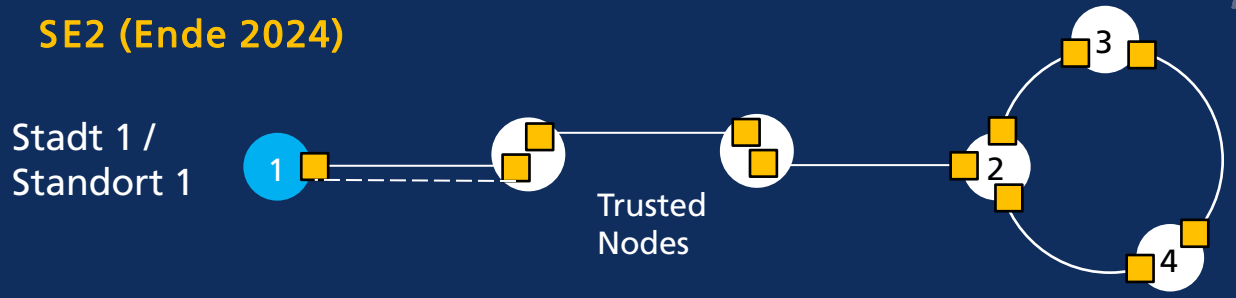
Standort 2

Ionenfalle / stationäres QuBIT

QuNET+ „KMS“ (tbd)

QuNET+ ML

### SE2 (Ende 2024)

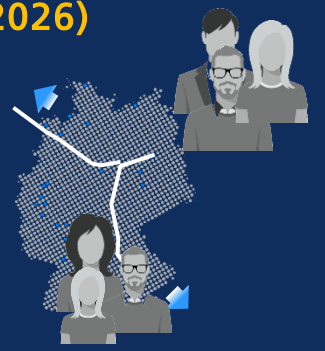



Stadt 2 / Standorte 2, 3, …

optimierte Topologie, Stern/Ring, Skizze als Beispiel, Einsatz TOGS / QuBUS

### SE4 (Ende 2026)

Endnutzer-
zu-Endnutzer





Fraunhofer DLR MAX-PLANCK-GESELLSCHAFT

# Schlüsselexperimente: Timeline

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

QuNET

2020 2021 2022 2023 2024 2025 2026

QuNET (SE1/2, Vorbereitung SE3/4) (SE3/4) Nach QuNET

vorbereitende Arbeiten

SE4*: Access Network / Endnutzer

SE3*: Mobile Knoten für lange Distanzen

SE2: Intercity backbone mit >=3 Access-Points

Demo in Bonn (BSI/BMBF) (SE0)

SE1: Metronetz: Ad-Hoc QKD (free-space/faser)

QuNET+ ML

QuNET+ XY

QuNET+ XY

QuNET+ XY

QuNET+ RECONNAITRE

KEEQUANT

Startups

Szenario III Multi-User-Netze

Szenario II Multi-Point-QKD

Szenario I Point-to-Point-QKD

Bewertungskompetenz / Rollout




* vorbereitende Arbeiten zu diesem Experiment sind im Arbeitsplan dargestellt. Die Demonstration fällt in die anschließende Phase nach Projektjahr 4, ist also nicht Teil des hier dargestellten Verbundvorhabens (jedoch Teil der QuNET Initiative).

DLR MAX-PLANCK-GESELLSCHAFT Fraunhofer

# Zwischenresümee

## Zuletzt & was kommt jetzt?

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Bisher:

- Was sind die Ziele QuNETs, und wer sind wir?
- Was sind die bisherigen und geplanten Beiträge & Aktivitäten der Kerninstitute (Hinweis: Mehr Informationen hierzu haben Sie in den Vorab-Slides erhalten)
- Was sind die Fehlbedarfe?

Jetzt:

- **Hintergrund für die Einbindung in QuNET: Projektstruktur**
- **Worauf lässt man sich ein? (QuNET-Struktur: Einbindung, Fachgruppen/Szenariogruppe)**
- **Wie kann man dazu beitragen / sich einbringen? (Prozess)**

# QuNET Projektstruktur

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung