Deploying QKD in Network Layer VPN Infrastructures

13 July, 2022

Prof. Dr.-Ing. Günter Schäfer, M. Sc. David Schatz, M. Sc. Friedrich Altheide

The SPIRIT of science

TECHNISCHE UNIVERSITÄT ILMENAU

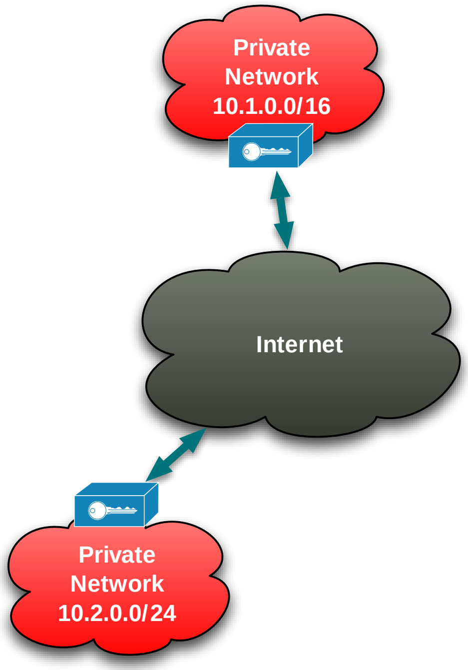
Roadmap

1. Network layer VPNs: Scenarios, requirements & current solutions
2. Challenge: How to defeat quantum computing attackers?
3. Emerging QKD standards: Overview and reflection
4. Integration of QKD & VPN Technology: An IT security guided approach
5. Conclusions

Network Layer VPN Infrastructures (1)

Scenario:

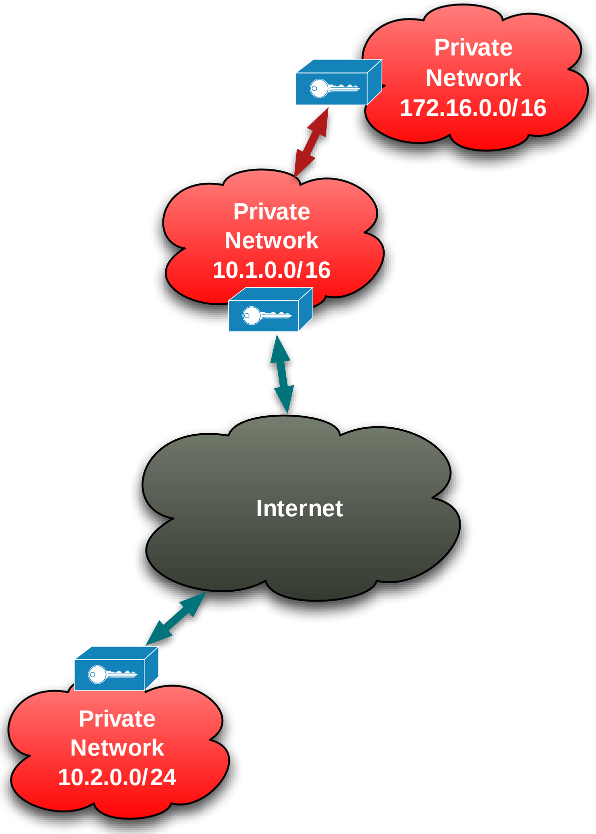
- VPN gateways and mobile workers connect internal networks over untrustworthy networks
- Smartcards used as trust anchors
- Public & private IP address ranges (IPv4 or IPv6)



Network Layer VPN Infrastructures (1)

Scenario:

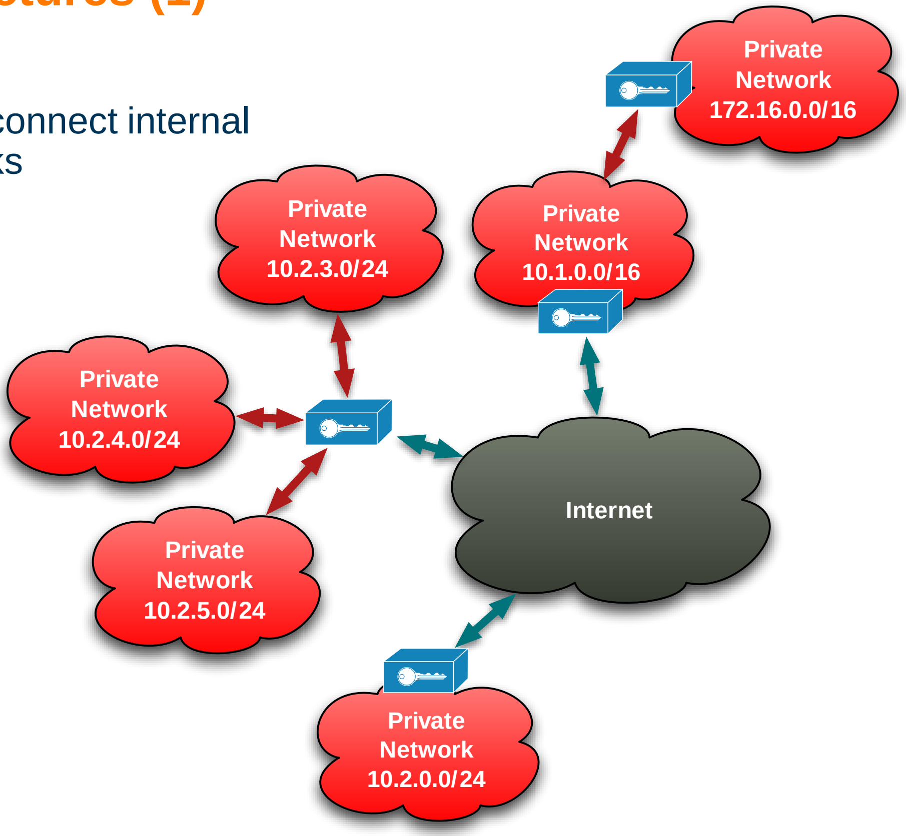
- VPN gateways and mobile workers connect internal networks over untrustworthy networks
- Smartcards used as trust anchors
- Public & private IP address ranges (IPv4 or IPv6)
- Nested networks



Network Layer VPN Infrastructures (1)

Scenario:

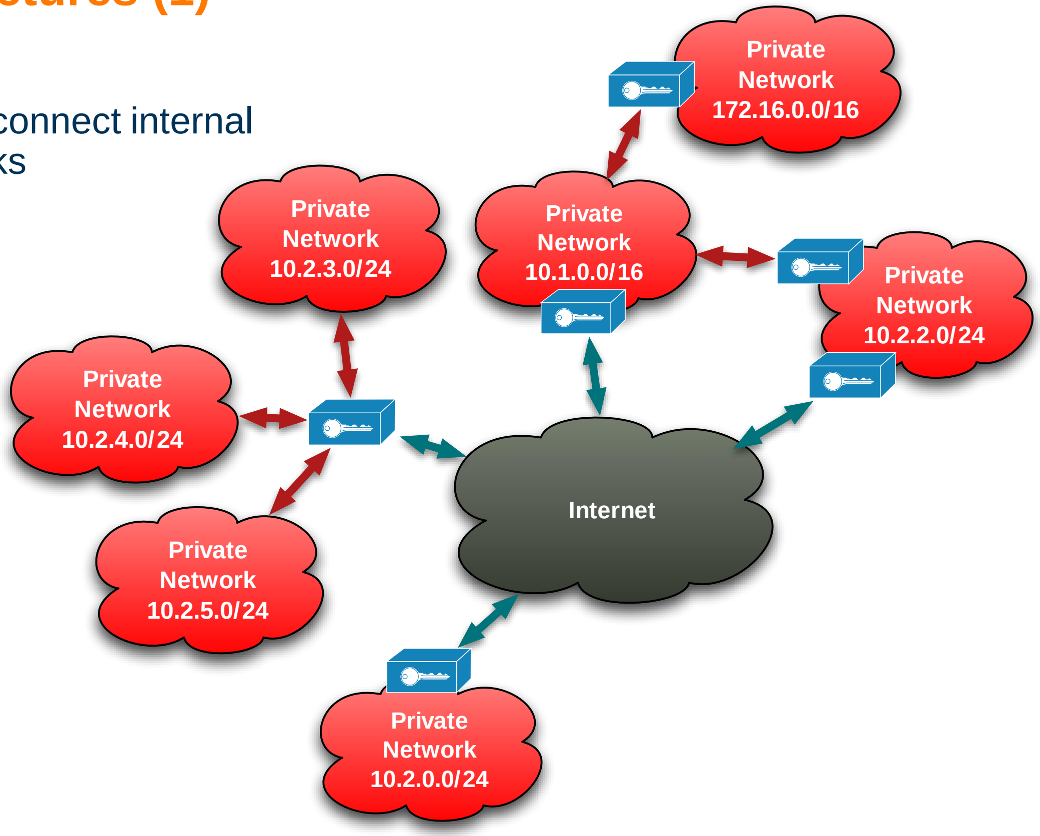
- VPN gateways and mobile workers connect internal networks over untrustworthy networks
- Smartcards used as trust anchors
- Public & private IP address ranges (IPv4 or IPv6)
- Nested networks
- Multiple networks per gateway



Network Layer VPN Infrastructures (1)

Scenario:

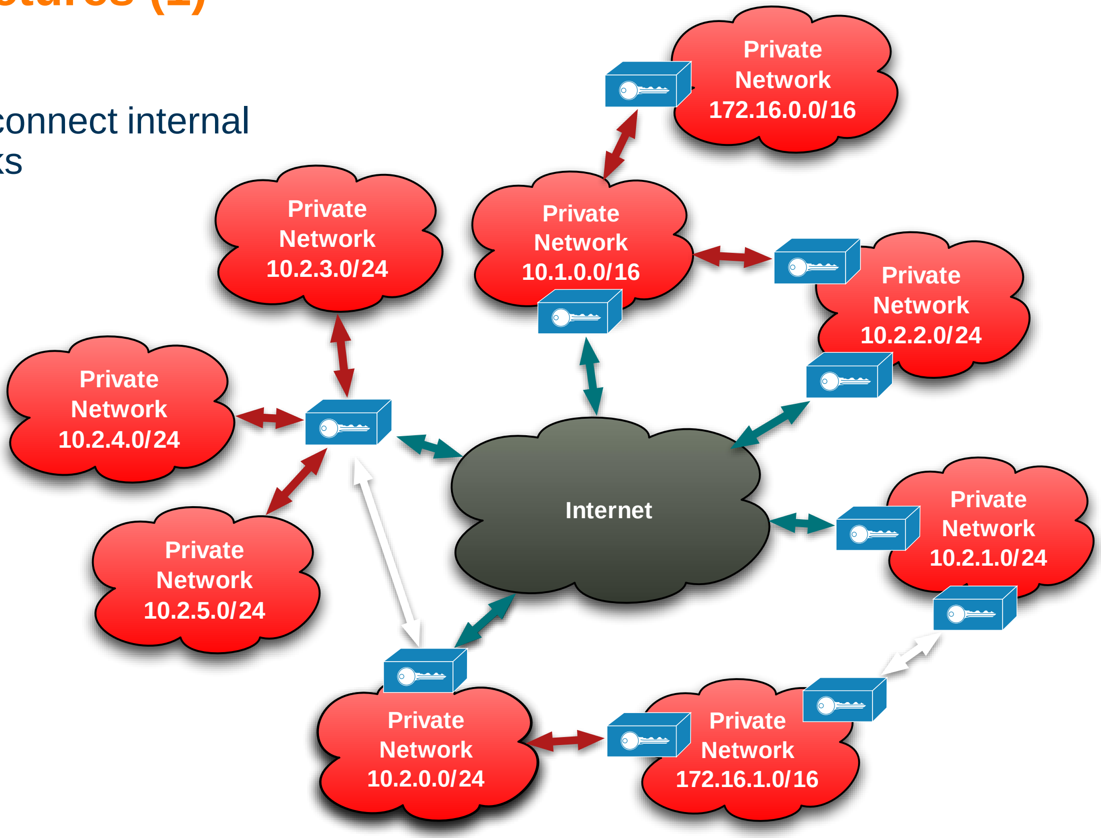
- VPN gateways and mobile workers connect internal networks over untrustworthy networks
- Smartcards used as trust anchors
- Public & private IP address ranges (IPv4 or IPv6)
- Nested networks
- Multiple networks per gateway
- Multiple gateways per network



Network Layer VPN Infrastructures (1)

Scenario:

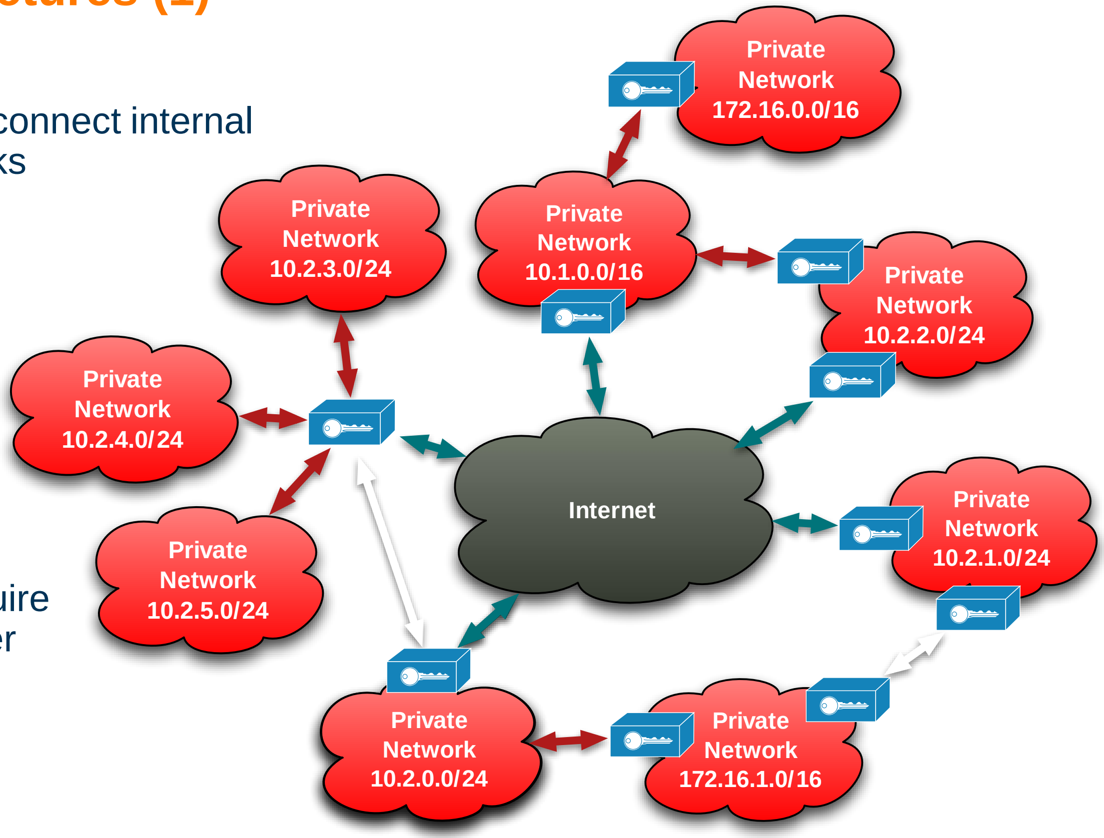
- VPN gateways and mobile workers connect internal networks over untrustworthy networks
- Smartcards used as trust anchors
- Public & private IP address ranges (IPv4 or IPv6)
- Nested networks
- Multiple networks per gateway
- Multiple gateways per network
- Cycles in the network (required for robustness and handling load!)



Network Layer VPN Infrastructures (1)

Scenario:

- VPN gateways and mobile workers connect internal networks over untrustworthy networks
- Smartcards used as trust anchors
- Public & private IP address ranges (IPv4 or IPv6)
- Nested networks
- Multiple networks per gateway
- Multiple gateways per network
- Cycles in the network (required for robustness and handling load!)
- Some sites with many networks require advanced load balancing and failover mechanisms

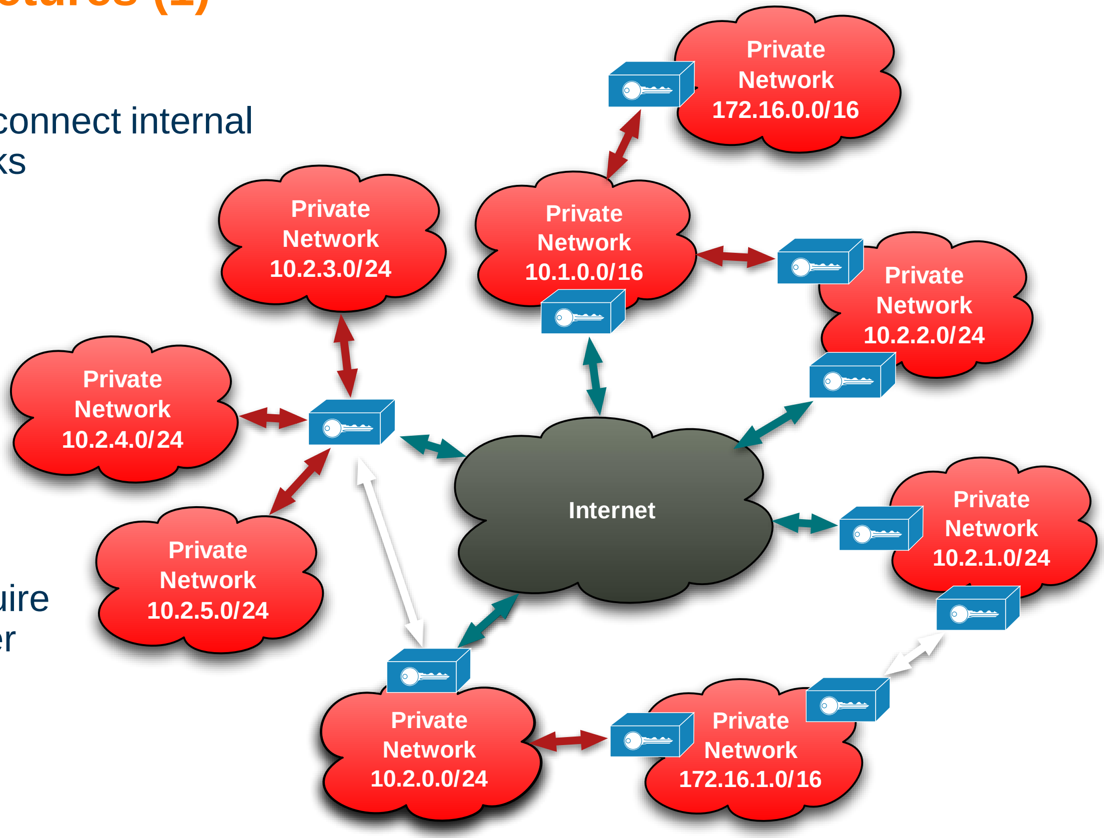


Network Layer VPN Infrastructures (1)

Scenario:

- VPN gateways and mobile workers connect internal networks over untrustworthy networks
- Smartcards used as trust anchors
- Public & private IP address ranges (IPv4 or IPv6)
- Nested networks
- Multiple networks per gateway
- Multiple gateways per network
- Cycles in the network (required for robustness and handling load!)
- Some sites with many networks require advanced load balancing and failover mechanisms

⇒ **High complexity!**



Network Layer VPN Infrastructures (2)

Customer expectations are simple:

- BSI-compliant crypto-processing at line speed or at least at well-defined speeds
- Handling of appliances as good/bad as other networking equipment:
  Robustness, management, enrollment
- Behave as transparently as possible
- Important VPN properties: scalability, agility, robustness

Key enablers to implement secure, scalable and robust VPNs:

- Avoid centralized components
- Use as few security associations (SAs) as possible (SA establishment is expensive!)
  - VPN gateways implement an overlay network/graph (gateway = node, SA = link)
  - Use tunneled SAs to guarantee end-to-end security (some gateways might be compromised)
- Keep (overlay) topology knowledge local
- Automatic configuration as far as possible (by “control algorithm”)

Network Layer VPN Infrastructures (3)

Further required for scenarios with enhanced needs for protection (e.g., “GEHEIM”):

- Security hardening of components, e.g., regarding:
  - Side-channel attacks
  - Minimizing trusted computing base (TCB)
  - Tamper-proofing
- Approval according to protection profile(s)

How to Overcome "Quantum Threat" to Classical Asymmetric Cryptography?

Two main directions:

- Post Quantum Cryptography (PQC)
  - Requires: Longer keys, longer messages and more computation (→ smart cards?)
  - Still raises concerns regarding maturity with respect to cryptanalysis
  - Required in the long run, but maybe not yet ready to be used alone
- Quantum Key Distribution (QKD)
  - Can "physically" guarantee confidentiality (but only after out-of-band authentication!)
  - Works only over "direct" medium (fiber, air) within limited reach (~100 km)

⇒ **Requires concepts for networking QKD-enabled devices**

Open challenges:

- How to do this without unnecessarily "reinventing wheels" (→ established VPN technology)?
- How to reduce efforts for hardening "QKD networking"-related software components?
- How can security be increased between red networks with no direct QKD link?
- How can security be increased for red networks with no QKD link at all?

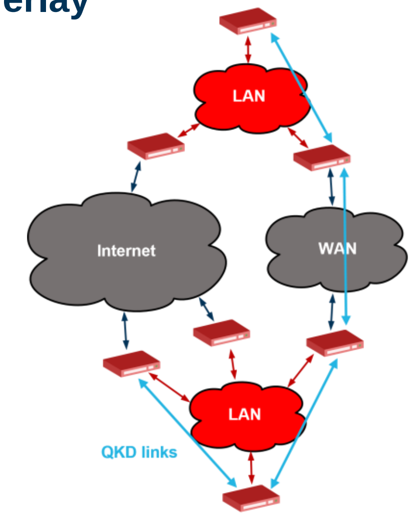
Implications for QKD Integration

At first glance: None!

- QKD only affects confidentiality, integrity, availability properties of certain links
- “Buried” in layers below

At second glance: We need to use the keys for establishing SAs in the overlay

- Secure interface between QKD devices and VPN gateways required
- Preferably integration of QKD keys in established protocols, e.g., IKEv2 (instead of a complete redesign)

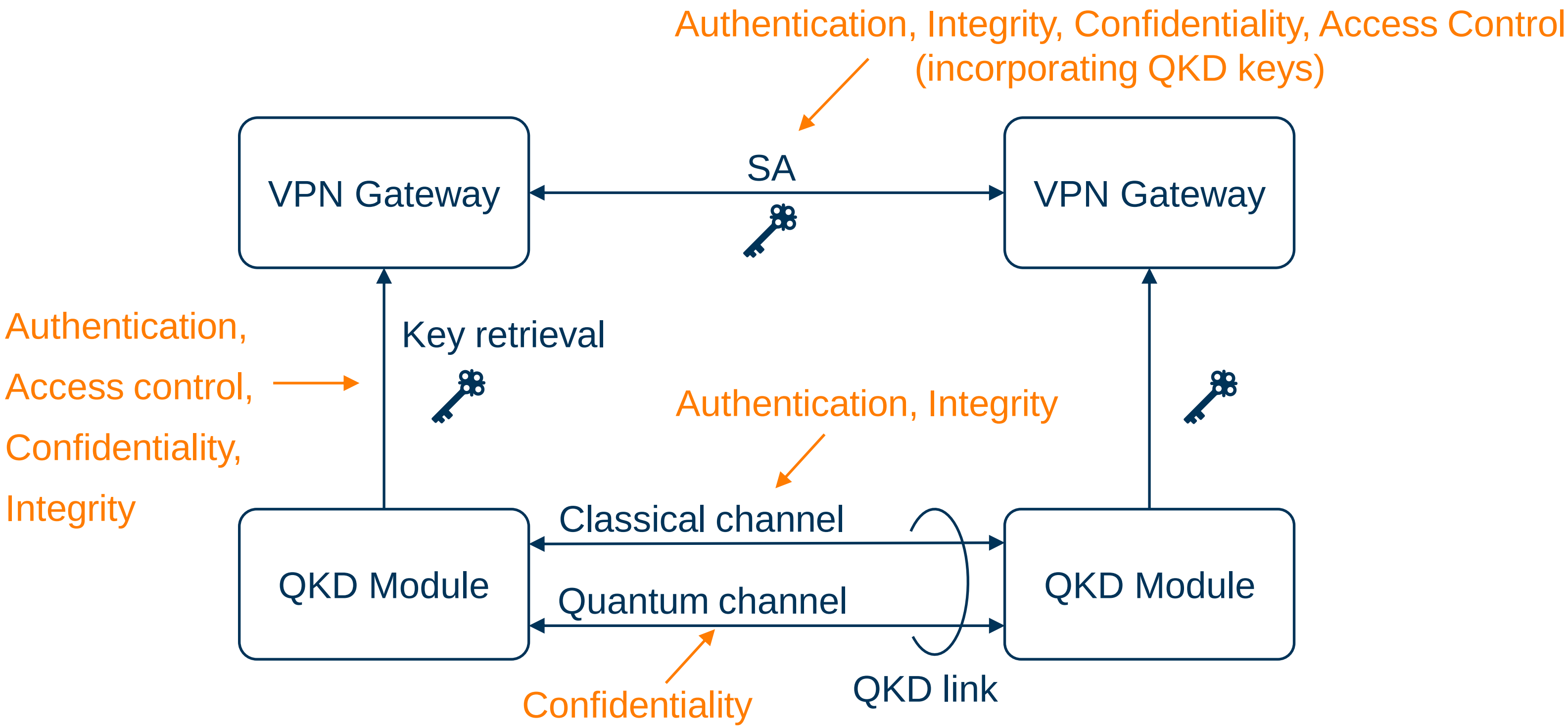


Broader view: Impact in heterogenous infrastructures?

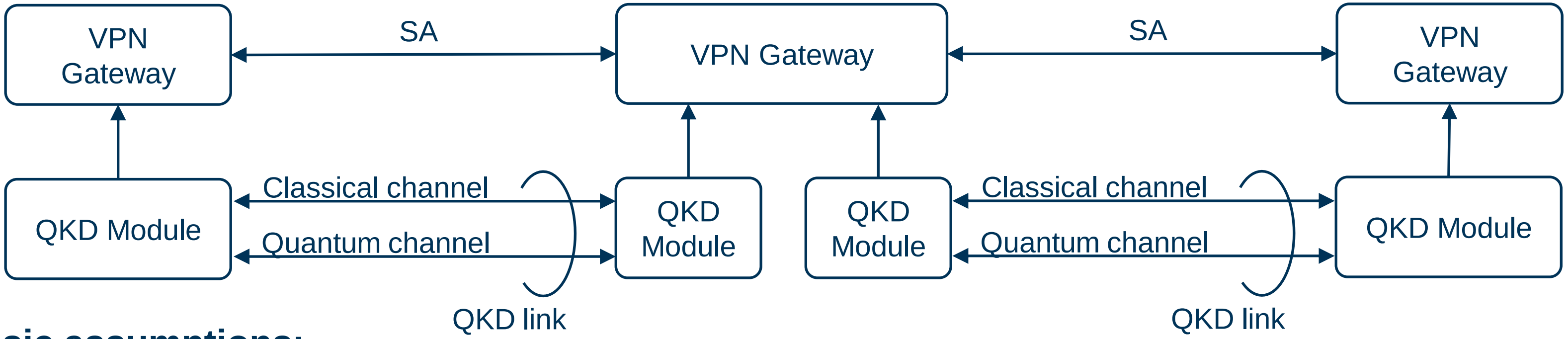
- Only some links have QKD (due to limited reach, costs)
- Benefit of QKD to the overall security for arbitrary SAs?
  - How to quantify benefit?
  - How to maximize benefit?

Required Security Services

Abstract, high-level view of QKD link integration:



QKD Network Security Considerations



Basic assumptions:

- Authentication needs to be realized with combination of PQC and classical cryptography
- Symmetric cryptography with sufficiently long keys (e.g., ≥ 256 bit) can not be broken
- It is impossible to eavesdrop on a “securely” authenticated QKD link
- It is rather easy to eavesdrop on individual classical links
- With growing network size, it gets harder to always eavesdrop on all classical links
- It is not impossible to compromise individual VPN gateways / QKD modules (but high effort!)
- The more complex a solution is, the easier it is to compromise

Emerging Standards: ITU-T Y.3800 – Y.3805 1/2

Scope: QKD networks

- Idea: Transparently extend the reach of QKD by relaying keys via “trusted” nodes
- Main contribution: Reference architecture(s)

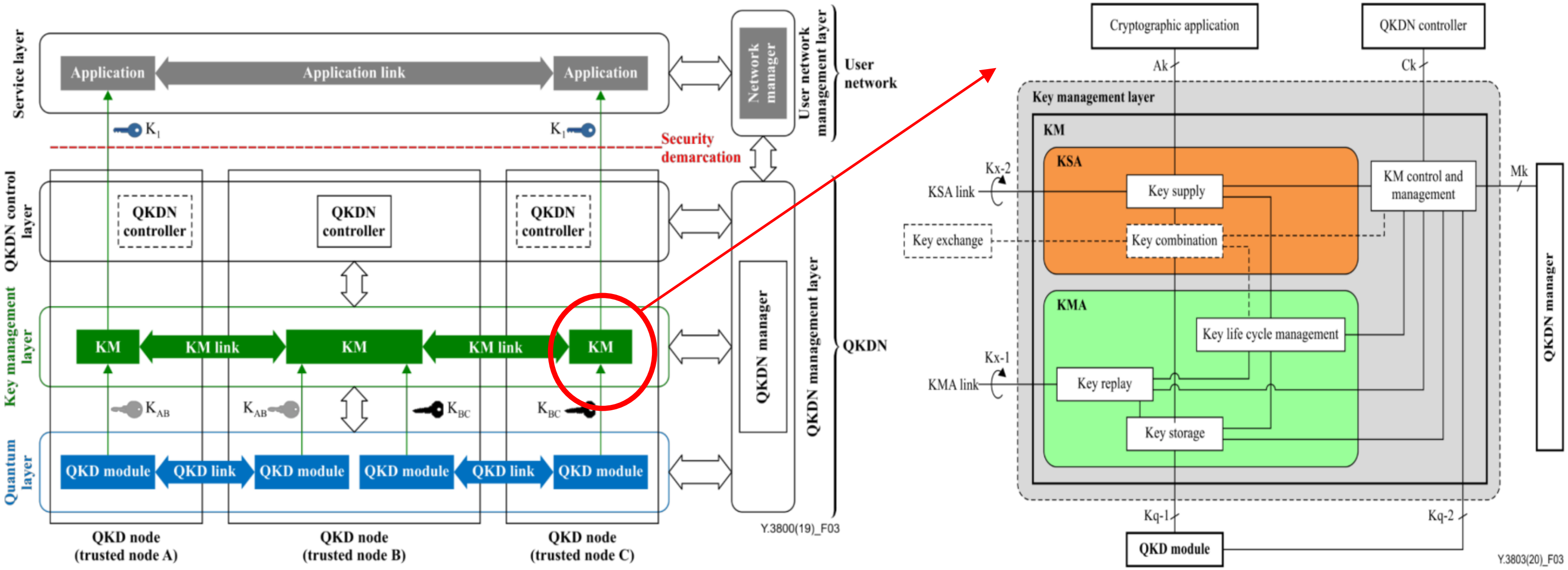


Figure source: [Y.3800, Y.3803]

Emerging Standards: ITU-T Y.3800 – Y.3805 2/2

Discussion:

- No specific protocols → No interoperability, implementation complexity "hidden"
- "Standard Writer's Standard"?
  - ~36 Functional Requirements with 9 notes [ITU-T Y.3801]
  - ~32 Functional Elements, ~22 Reference Points [ITU-T Y.3802]
  - > 50 Functions [ITU-T Y.3804]

  → overly complicated?
- Security services: Identified, but very little information provided on what concrete security objectives need to be ensured and how this is supposed to be realized:
  - "[Security] [d]etails are outside the scope of this Recommendation" [ITU-T Y.3801, Y.3802, Y.3804, Y.3805]
  - "[…] security requirements described in [ITU-T X.1710], [ITU-T Y.3801] and [ITU-T Y.3802] and general network security requirements and mechanisms in IP-based networks described in [ITU-T Y.2701] and [ITU-T Y.3101] are recommended to be applied"

  → How to ensure secure implementations with these recommendations?

Figure source: [Y.3800, Y.3803]

Gall's Law

John Gall (1925 –2014), pediatrician and author

- Most famous book: *"General Systemantics: An Essay On How Systems Work, And Especially How They Fail..."* (1975)
  (Third edition, entitled "The Systems Bible" published in 2002)

- *"A complex system that works is invariably found to have evolved from a simple system that worked.*
  A complex system designed from scratch never works and cannot be patched up to make it work.
  You have to start over with a working simple system." (1975, p. 71)

- In security, we are not only concerned with systems simply "working", but to ensure that they do not have unintended vulnerabilities
  - This is even harder to achieve!

Emerging Standards: ETSI GS QKD 004, 014

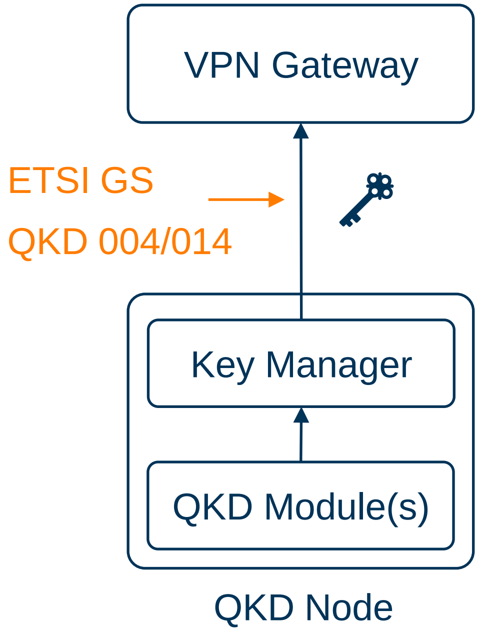
Scope: Key retrieval in QKD networks

ETSI GS QKD 014

- State of the art in commercially available products
- REST-based HTTP API
- Security services implemented by PKI-based TLS
  - Does not match the security level of QKD
  - Overall huge TCB: ~500k lines of code dependencies for client and server each (using well established Rust libraries)

ETSI GS QKD 004

- Sleeker design compared to ETSI GS QKD 014 → Right direction
- But: Underspecified (e.g., encoding on wire) → Interoperability?



Emerging Standards: ETSI GS QKD 015, 018

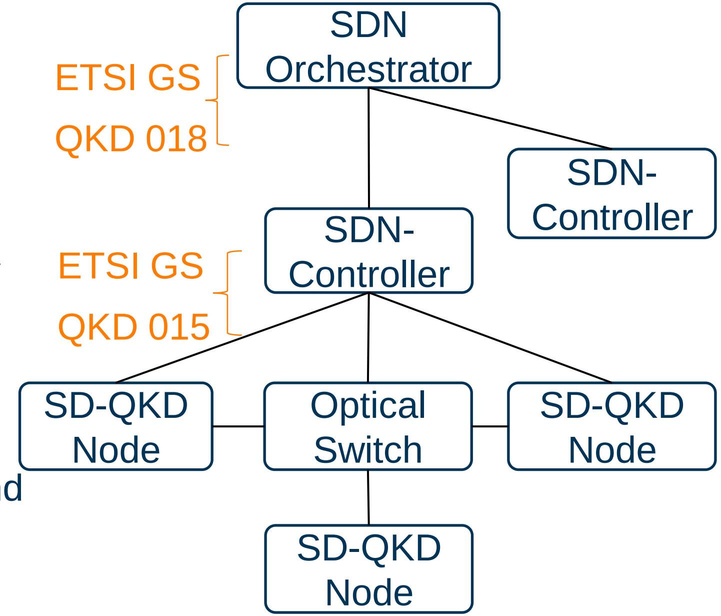
Scope: Management & monitoring of QKD nodes

ETSI GS QKD 015

- Central management and on demand configuration of QKD nodes and “lightpaths” using SDN
- Dynamically configuring trusted nodes to increase reachability
  → Introduces central weak point (SDN controller)

ETSI GS QKD 018

- Introduces SDN orchestrator for multi-domain management and monitoring
  - But: What is a domain? How separated?



The SPIRIT of science
TECHNISCHE UNIVERSITÄT ILMENAU

Emerging Standards: Reflection

Common conception/objective: “Standalone” QKD networks?

- Hope: Maximizes transparency for (generic) key consumers

Not optimally suited in the context of existing VPN infrastructures

- Routing, key management, authentication, and integrity implemented on two layers (QKD and VPN) → Increased complexity and larger TCB
- Lack of standardization for many interfaces and implementation of security services (e.g., authentication on classical channel of QKD links)
  - → Proprietary protocols and implementations
  - → Additional effort for hardening and approval of QKD nodes software components
- “Trusted” nodes not satisfying (or even prohibitive?) in VPNs with enhanced needs for protection

Integrated approach better suited?

How to maximize the benefit of QKD without solely relying on trusted nodes?

Excursion: Software Vulnerabilities

Some examples:

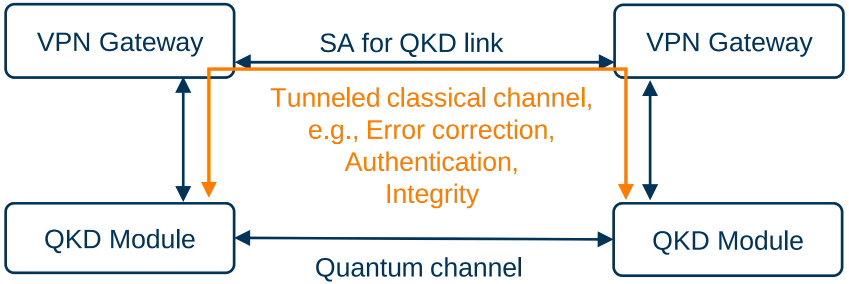
- Heartbleed [CVE-2014-01600]: Memory leak in the `openssl` implementation of the TLS heartbeat extension → Potentially leaked many long-term secret keys
- Log4Shell [CVE-2021-44228]: Vulnerability in “harmless” dependency (logging framework) → Allowed remote code execution for nearly ten years
- And countless more

Implications:

- Avoid (designing and) implementing complex protocols from scratch
- Keep TCB as small as possible

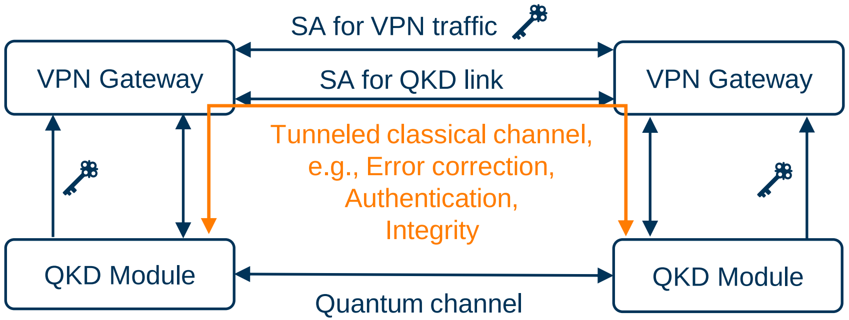
Integrated Approach: Direct QKD Link

- Additional SA for each QKD link, established using PQC/pre-shared keys (PSKs)
- Tunnel classical channel (e.g., error correction) via VPN gateways and additional SA
- Options for security services between QKD module and VPN gateway: PQC, PSKs, “physical means”



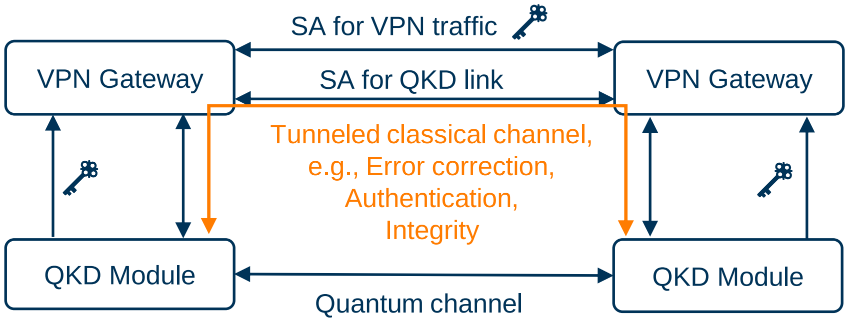
Integrated Approach: Direct QKD Link

- Additional SA for each QKD link, established using PQC/pre-shared keys (PSKs)
- Tunnel classical channel (e.g., error correction) via VPN gateways and additional SA
- Options for security services between QKD module and VPN gateway: PQC, PSKs, “physical means”
- Use QKD key to establish SA for “normal” VPN traffic (include in key derivation)
- Traffic secured by symmetric cryptography as usual (e.g., AES, …)



Integrated Approach: Direct QKD Link

- Additional SA for each QKD link, established using PQC/pre-shared keys (PSKs)
- Tunnel classical channel (e.g., error correction) via VPN gateways and additional SA
- Options for security services between QKD module and VPN gateway: PQC, PSKs, “physical means”
- Use QKD key to establish SA for “normal” VPN traffic (include in key derivation)
- Traffic secured by symmetric cryptography as usual (e.g., AES, …)

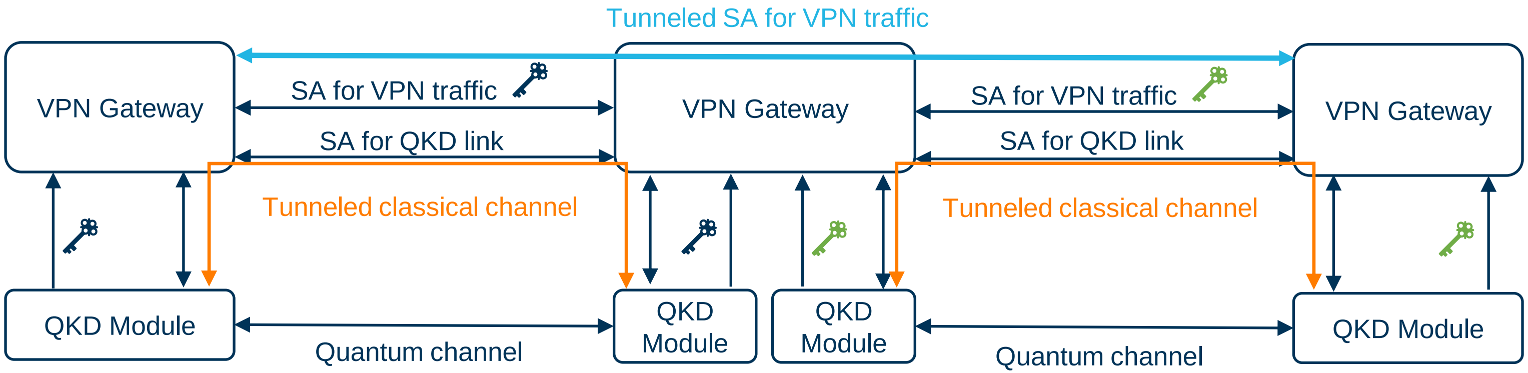


→ Reduced attack surface on QKD modules (no classical communication via public channels)
→ Reduced complexity of QKD modules (no authentication with other modules)

Integrated Approach: Multi-hop QKD

Approach:

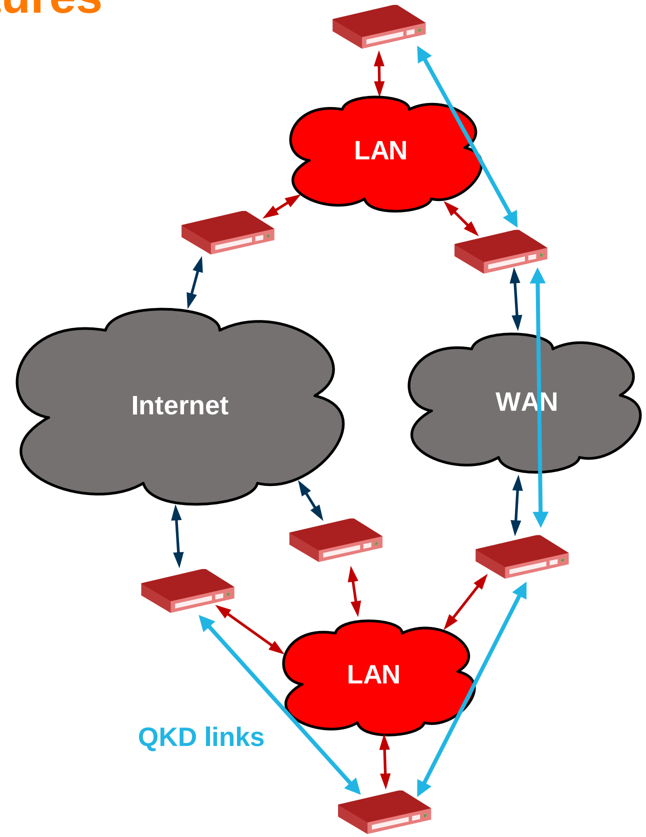
- Establish “tunneled” SA, hop-by-hop protected by existing SAs with direct access to QKD links
- End-to-end authentication and key exchange: PQC/classical cryptography
- Optimization: Re-route (shortcut) VPN traffic after successful authenticated key exchange



Discussion:

- Same (or better?) end-to-end security properties compared to QKD network with trusted nodes
- Reduced complexity and TCB (use established VPN technologies for multi-hop key management)

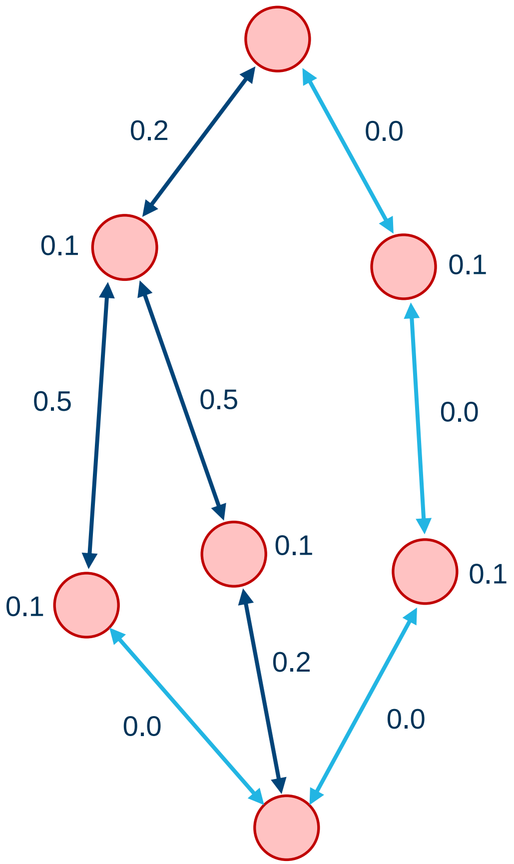
Integrated Approach: Heterogeneous Infrastructures



Integrated Approach: Heterogeneous Infrastructures

Approach:

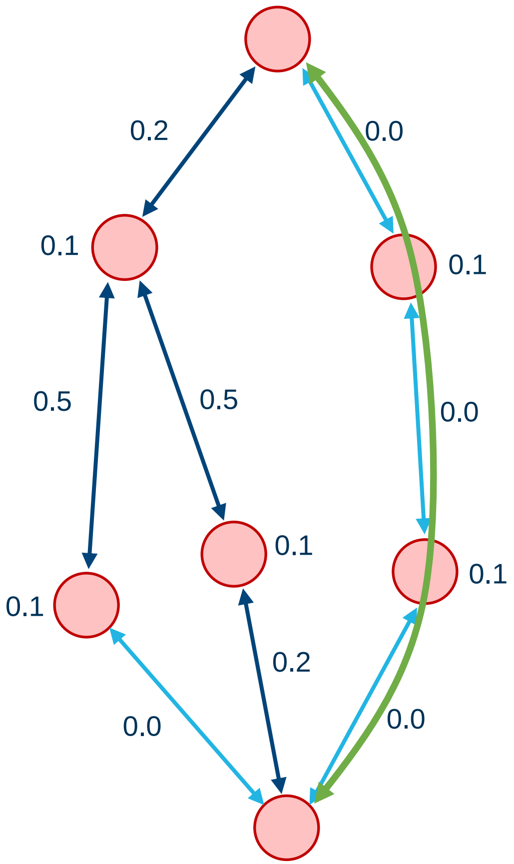
- Graph representation of existing VPN overlay topology
- Augment probability of node/edge compromise



Integrated Approach: Heterogeneous Infrastructures

Approach:

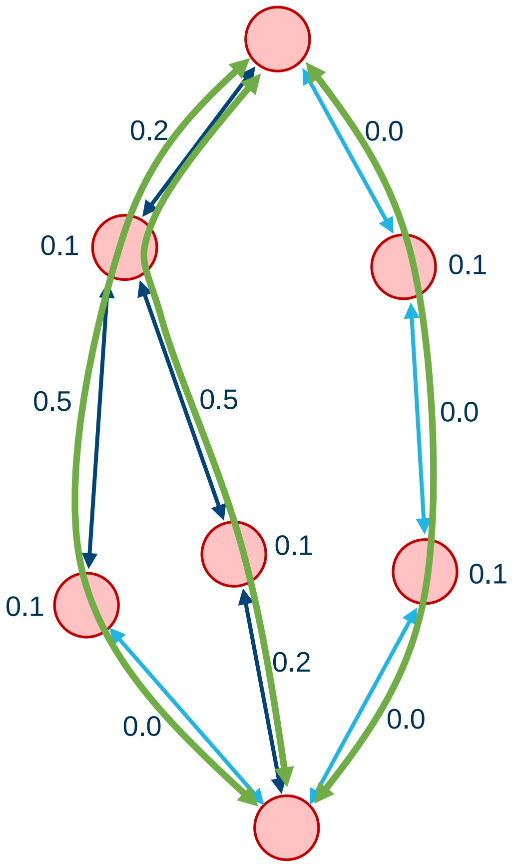
- Graph representation of existing VPN overlay topology
- Augment probability of node/edge compromise
- Establish tunneled SA, e.g., on path with lowest probability of compromise



Integrated Approach: Heterogeneous Infrastructures

Approach:

- Graph representation of existing VPN overlay topology
- Augment probability of node/edge compromise
- Establish tunneled SA, e.g., on path with lowest probability of compromise
- Reinforce key by additional key exchanges
  - E.g., $K = H(S_1, S_2, \ldots, S_n)$
  - Key shares S_i established over diverse paths and at various times



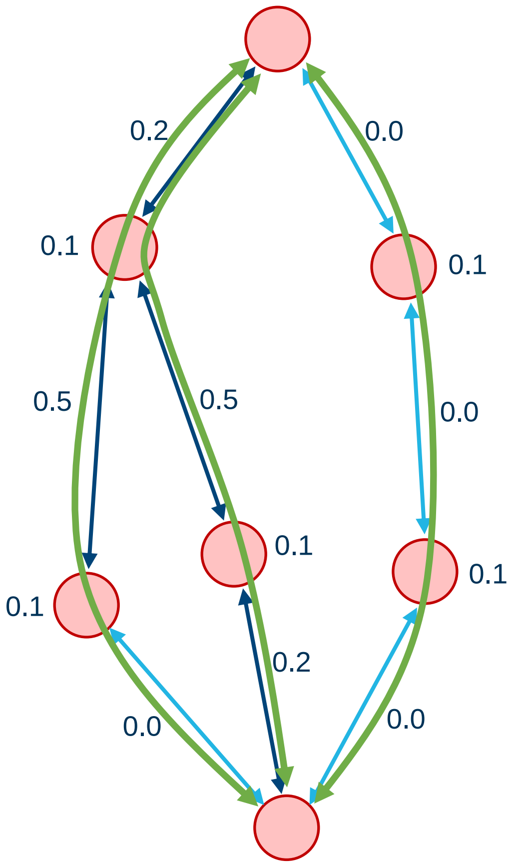
Integrated Approach: Heterogeneous Infrastructures

Approach:

- Graph representation of existing VPN overlay topology
- Augment probability of node/edge compromise
- Establish tunneled SA, e.g., on path with lowest probability of compromise
- Reinforce key by additional key exchanges
  - E.g., $K = H(S_1, S_2, \ldots, S_n)$
  - Key shares S_i established over diverse paths and at various times

Discussion:

- Increases effort for attackers (must attack at all paths/times)
- Reduces dependence on “trusted” nodes
- Model is first step towards quantifying QKD gain in heterogeneous infrastructures

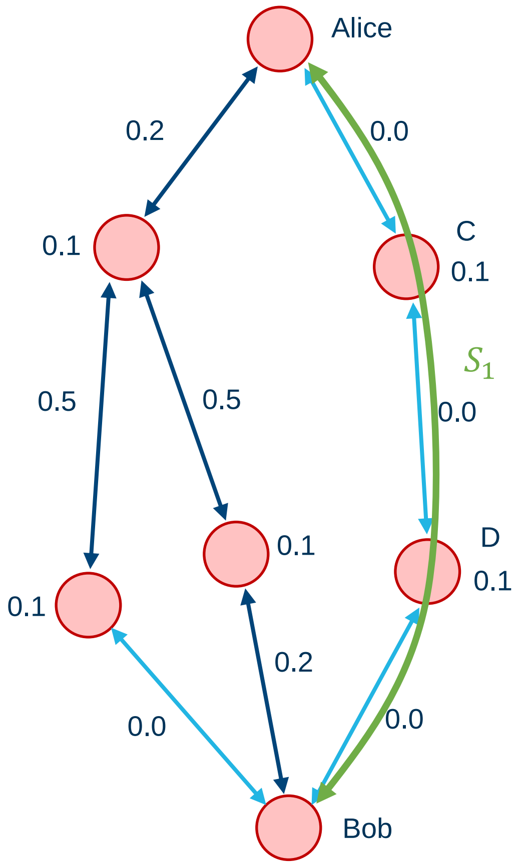


Quantifying the Security of Keys (1)

Scenario 1: Multi-hop QKD

- Establish key $K_1 := S_1$ via multi-hop QKD path

$$
\begin{aligned}
Pr(K_1 \text{ secure}) &= Pr(C \text{ secure}) \times Pr(D \text{ secure}) \\
&= (1 - Pr(C \text{ insecure})) \times (1 - Pr(D \text{ insecure})) \\
&= (1 - 0.1) \times (1 - 0.1) = 0.81
\end{aligned}
$$



Quantifying the Security of Keys (1)

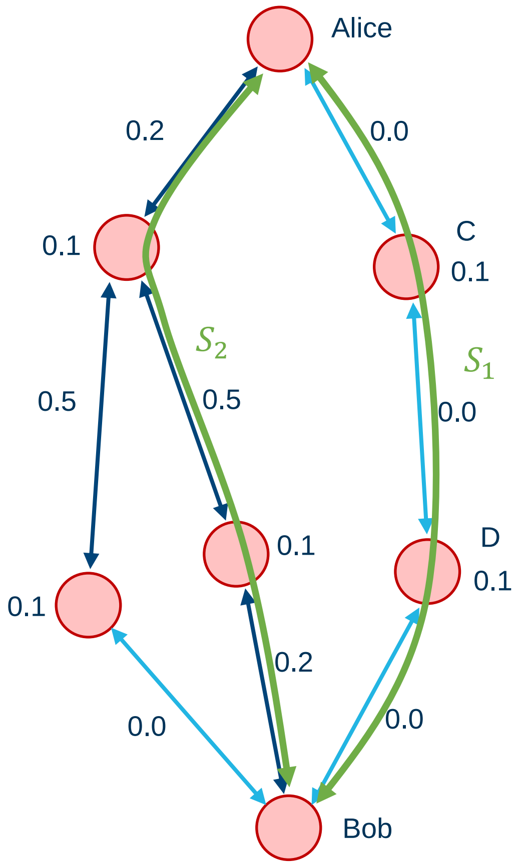
Scenario 1: Multi-hop QKD

- Establish key $K_1 := S_1$ via multi-hop QKD path

$$\begin{aligned} Pr(K_1 \text{ secure}) &= Pr(C \text{ secure}) \times Pr(D \text{ secure}) \\ &= (1 - Pr(C \text{ insecure})) \times (1 - Pr(D \text{ insecure})) \\ &= (1 - 0.1) \times (1 - 0.1) = 0.81 \end{aligned}$$

- Reinforce key with $S_2 \rightarrow K_2 := H(K_1, S_2)$
- $Pr(K_2 \text{ secure}) = 1 - Pr(S_1 \text{ insecure}) \times Pr(S_2 \text{ insecure})$

$$\begin{aligned} &= 1 - (1 - 0.81) \times (1 - 0.8 \times 0.9 \times 0.5 \times 0.9 \times 0.8) \\ &\approx 0.86 \end{aligned}$$



Quantifying the Security of Keys (1)

Scenario 1: Multi-hop QKD

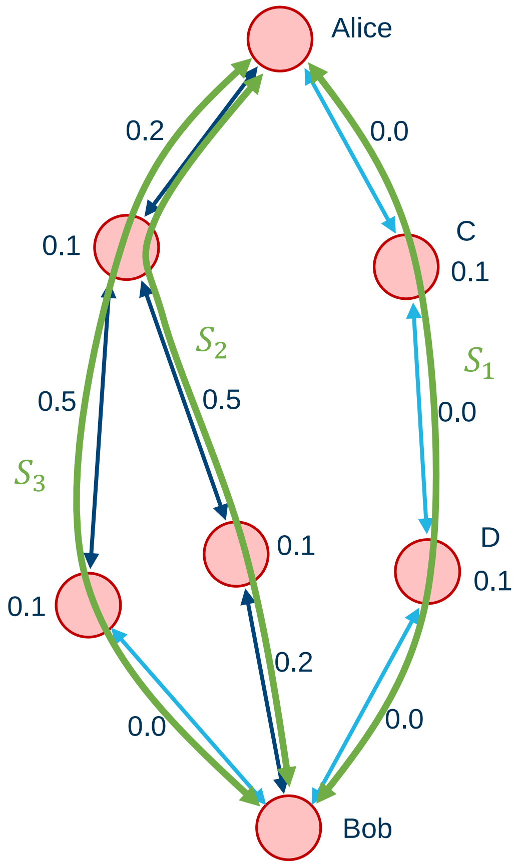
- Establish key $K_1 := S_1$ via multi-hop QKD path

$$Pr(K_1 \text{ secure}) = Pr(C \text{ secure}) \times Pr(D \text{ secure})$$
$$= (1 - Pr(C \text{ insecure})) \times (1 - Pr(D \text{ insecure}))$$
$$= (1 - 0.1) \times (1 - 0.1) = 0.81$$

- Reinforce key with $S_2 \rightarrow K_2 := H(K_1, S_2)$
- $Pr(K_2 \text{ secure}) = 1 - Pr(S_1 \text{ insecure}) \times Pr(S_2 \text{ insecure})$

$$= 1 - (1 - 0.81) \times (1 - 0.8 \times 0.9 \times 0.5 \times 0.9 \times 0.8)$$
$$\approx 0.86$$

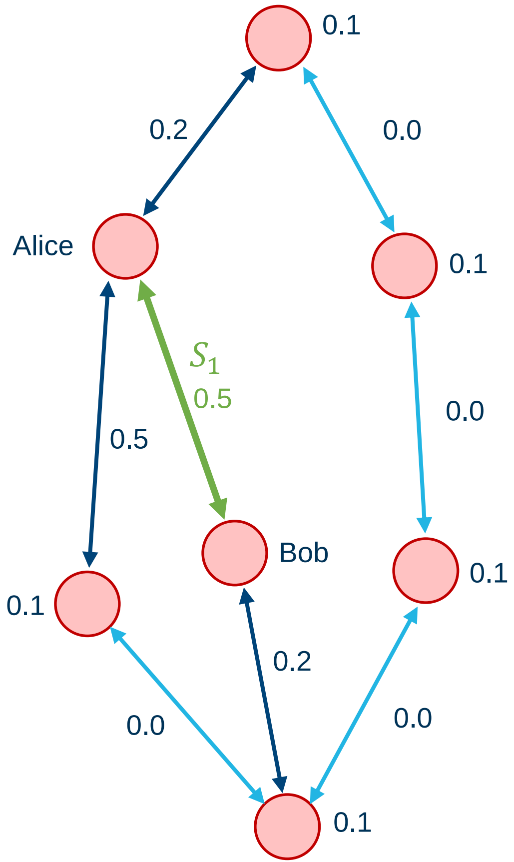
- Further reinforce key with $S_3 \rightarrow K_3 := H(K_2, S_3)$
- $Pr(K_3 \text{ secure}) = \ldots \approx 0.90$
  (Note: Calculation more complex due to non-disjoint paths)



Quantifying the Security of Keys (2)

Scenario 2: No direct access to QKD

- Initial direct SA with key $K_1 := S_1$
- $Pr(K_1 \text{ secure}) = 0.5$

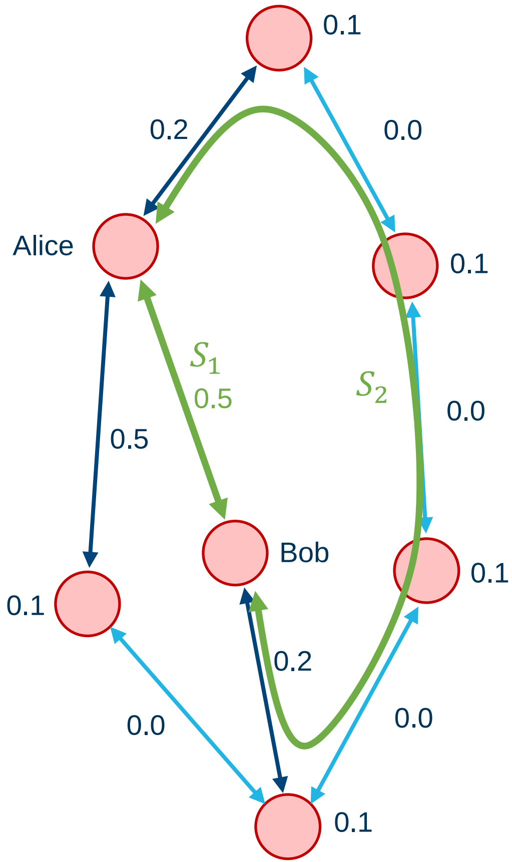


Quantifying the Security of Keys (2)

Scenario 2: No direct access to QKD

- Initial direct SA with key $K_1 := S_1$
- $Pr(K_1 \text{ secure}) = 0.5$

- S_2 better initial choice?
-

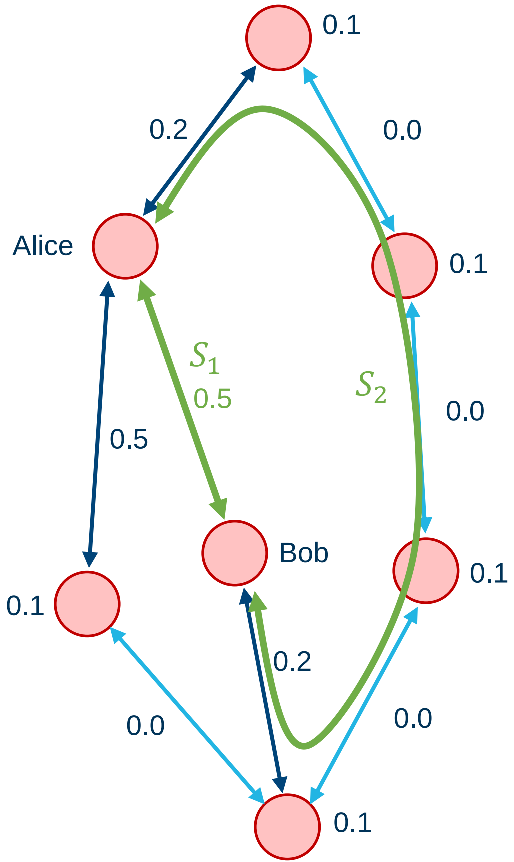


Quantifying the Security of Keys (2)

Scenario 2: No direct access to QKD

- Initial direct SA with key $K_1 := S_1$
- $Pr(K_1 \text{ secure}) = 0.5$

- S_2 better initial choice?
- $Pr(S_2 \text{ secure}) = 0.8 \times 0.9^4 \times 0.8 \approx 0.42$
  $\rightarrow$ No (path too long)

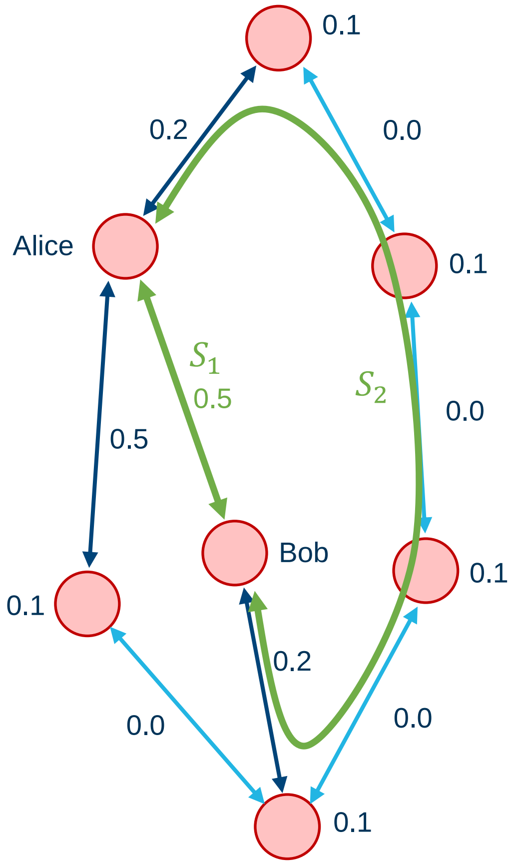


Quantifying the Security of Keys (2)

Scenario 2: No direct access to QKD

- Initial direct SA with key $K_1 := S_1$
- $Pr(K_1 \text{ secure}) = 0.5$

- S_2 better initial choice?
- $Pr(S_2 \text{ secure}) = 0.8 \times 0.9^4 \times 0.8 \approx 0.42$
  $\rightarrow$ No (path too long)
- Still: Reinforce key with $S_2 \rightarrow K_2 := H(K_1, S_2)$
- $Pr(K_2 \text{ secure}) \approx 1 - (1 - 0.5) \times (1 - 0.42) \approx 0.71$



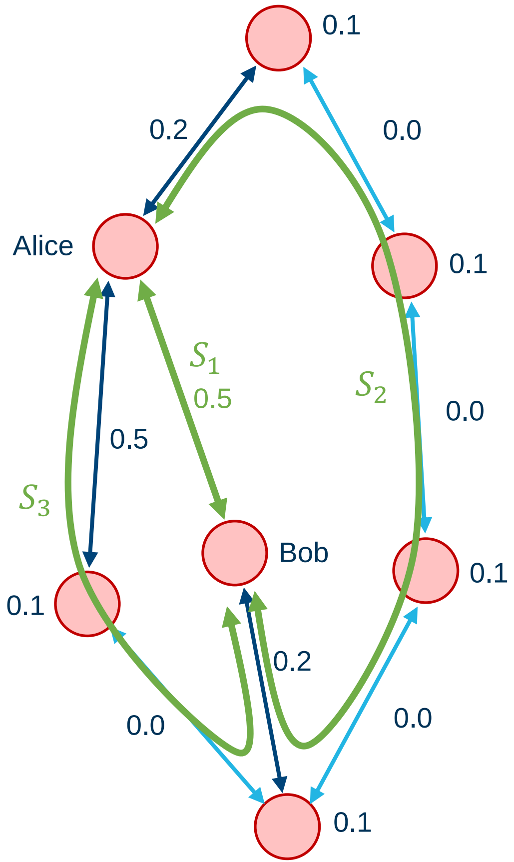
Quantifying the Security of Keys (2)

Scenario 2: No direct access to QKD

- Initial direct SA with key $K_1 := S_1$
- $Pr(K_1 \text{ secure}) = 0.5$

- S_2 better initial choice?
- $Pr(S_2 \text{ secure}) = 0.8 \times 0.9^4 \times 0.8 \approx 0.42$
  $\rightarrow$ No (path too long)
- Still: Reinforce key with $S_2 \rightarrow K_2 := H(K_1, S_2)$
- $Pr(K_2 \text{ secure}) \approx 1 - (1 - 0.5) \times (1 - 0.42) \approx 0.71$

- Further reinforce key with $S_3 \rightarrow K_3 := H(K_2, S_3)$
- $Pr(K \text{ secure}) = \ldots \approx 0.79$



Conclusion

- Security of existing VPN infrastructures threatened by quantum attackers
- One possible countermeasure: QKD
- QKD standards & commercially available products focus on “standalone” QKD networks
  - Not suited for deployment in VPN infrastructures
  - Significantly increase attack surface and TCB → Approval cumbersome
- Complexity of QKD deployment and management should be reduced by utilizing existing VPN technologies
  - Reuse existing and established VPN-Gateways to secure the classical channel between QKD devices
  - Established mechanisms for utilizing multi-hop QKD (routing, tunneled SAs)
- QKD on its own not sufficient (cost, reach) → PQC required in long-run for e2e security
- Multipath key exchange as an additional and orthogonal approach for quantum-safety

Thanks for listening!

firstname.lastname@tu-ilmenau.de | www.tu-ilmenau.de/telematik