Beyond the Central Server: End-to-End Protected Communication and Collaboration

AI-Driven Attacks and Quantum Risk, Design Principles, and Two Realized Technology Demonstrators: HeyAppPro and CollabNowPro

Beat W. Meier *

Author · Entrepreneur · Visionary · Engineer — beat-w-meier.ch, Switzerland

ARTICLE INFO

Article history:

Created on November 11, 2026

Data as of: November 11, 2026

Version 1.0

Sources: standards, government reports, statutes, peer-reviewed literature, vendor disclosures, and a code and test review of both projects

Keywords:

decentralized architecture

end-to-end encryption

anonymized network

segmented data storage

AI-driven vulnerability discovery

post-quantum transition

digital sovereignty

ABSTRACT

Three developments are changing the risk calculation for centrally operated digital services. AI systems now find and exploit software vulnerabilities at a pace that human review cannot match: 848 Linux kernel CVEs were published on a single day in August 2026, and one AI campaign produced 948 working privilege-escalation exploits for the same kernel. Quantum computing threatens the public-key methods that protect today's traffic, and encrypted data can be recorded now and decrypted later. Statutes such as the U.S. CLOUD Act give authorities access to data held by providers regardless of where the data center stands. All three pressures converge on the central platform that holds identities, content, keys, and metadata in one place. This study derives six design principles for an architecture that does not depend on such a platform and illustrates them with two technology demonstrators that exist as working software. HeyAppPro is a messenger without a subscriber registry that transports only end-to-end encrypted traffic over an anonymized network and stores messages for absent recipients as ciphertext on small, rotating groups of nodes. CollabNowPro unites mail, calendar, contacts, tasks, notes, files, and an AI assistant in one application that works against infrastructure the organization itself controls, reached through a private mesh. The study describes advantages and principles of operation, omits everything that would enable a reimplementation, and states the limits: neither demonstrator uses post-quantum algorithms yet, anonymity is not absolute, and independent security audits are outstanding.

Contact: beat-w-meier.ch/kontakt · © 2026 Beat W. Meier. All rights reserved.

Management Summary

For two decades, the standard home of digital communication has been the central platform. One operator runs the servers, keeps the accounts, stores the content, and holds the keys or at least the metadata. Whoever compromises that platform, technically, organizationally, or by legal order, reaches everything at once.

Three developments make this concentration more dangerous than before. First, AI systems have turned vulnerability discovery into an industrial process. Engineers who maintain the Linux kernel for a large cloud provider report that kernel CVEs rose from about two per week before 2024 to about sixteen per day, with 848 published on August 15, 2026 alone. [Q01] In November 2026, one AI vendor reported a single campaign that yielded 948 working exploits giving root access on Linux. [Q02]

Second, the U.S. National Institute of Standards and Technology (NIST) will deprecate today's quantum-vulnerable public-key cryptography after 2030 and disallow it after 2035, and it warns that

adversaries already collect encrypted data in order to decrypt it later. [Q03] Third, the CLOUD Act obliges providers under U.S. jurisdiction to disclose data in their possession, custody, or control regardless of whether the data are located inside or outside the United States. [Q04]

That the danger is real is shown by the incidents of 2026 alone. In Switzerland, records of more than 100,000 current and former federal employees were taken from a supplier of pension fund software. [Q05] In the United States, a medical technology manufacturer had tens of thousands of devices wiped in a single stroke [Q06], and the FBI recorded reported cybercrime losses of 20.9 billion U.S. dollars for 2025. [Q07]

The response proposed here does not try to harden the central platform further. It removes the platform from the path. Information travels end-to-end encrypted between the devices of the people involved, transport runs over an anonymized network that hides who is talking to whom, and whatever must be stored is segmented: no single system holds all data, and no storage location holds anything but ciphertext.

Key finding

HeyAppPro and CollabNowPro show that this architecture is not a research vision. Both exist as working software on real devices. HeyAppPro exchanges messages through a live fleet of nodes without any central subscriber registry. CollabNowPro operates mail, calendar, and collaboration data against the organization’s own servers, reached only through a private mesh. Both are technology demonstrators, not finished products: independent security audits, post-quantum cryptography, and full device acceptance are still outstanding.

The study names the price of the approach. An anonymized network makes traffic analysis costly, not impossible. Segmented storage tolerates failures and limits the damage of a compromise, but it does not survive a malicious majority of storage nodes. CollabNowPro still relies on servers, though they belong to the organization itself. And cryptography that is safe today must be replaced before large quantum computers arrive.

1. Mandate, Subject, and Scope

1.1 Research Questions

The study answers three questions. Which developments increase the risk of centrally operated communication and collaboration services? Which design principles follow for systems that are meant to remain confidential under these conditions? And how do the two technology demonstrators HeyAppPro and CollabNowPro implement these principles, with which advantages and which limits?

1.2 Method and Evidence Base

The threat analysis rests on official standards and government reports, statutory texts, peer-reviewed literature, conference material, and primary disclosures by vendors. Vendor statements are self-disclosures and are marked as such. Where an original vendor publication could not be retrieved directly, the study cites the trade publication that reports on it and says so in the reference. Recent incidents for which no official report exists yet are documented through established trade media.

The description of the two demonstrators is based on a review of their active source code repositories, requirement and architecture documents, progress records, and recorded test results, carried out on November 11, 2026. Statements about implementation status distinguish between three levels: implemented and observed on real devices, implemented and tested locally, and specified only. A design goal is never presented as a demonstrated property. No new tests were run for this study.

© 2026 Beat W. Meier · All rights reserved.

Status: Public.

1.3 Deliberate Abstraction

The study describes the problem, the design principles, and the way the demonstrators work in principle. It deliberately omits all information that would enable a reimplementation. This includes message formats and protocol flows, key hierarchies and derivations, timers, quotas and limits, the algorithms for node selection, admission, discovery, and storage placement, software libraries and versions, isolation configurations, and the operational topology. The names HeyAppPro and CollabNowPro are used as designations of technology demonstrators. The abstraction does not limit the verifiability of the argument, because the argument rests on published methods with known properties.

1.4 Terminology

End-to-end encryption means that only the devices of the communicating parties hold the keys needed to read content. An **anonymized network** is an overlay network that relays traffic through several independent stations in layered encryption, so that no single station knows both origin and destination. [Q08] **Metadata** are all circumstances of communication other than content: identities, contact relationships, times, sizes, and network addresses. **Segmented data storage** means that data are divided by function, owner, and location so that no single system contains a complete picture. A **private mesh** is an encrypted overlay network to which only individually admitted devices belong. A **technology demonstrator** is working software that proves the feasibility of a design without claiming product maturity.

2. The Changed Threat Landscape

2.1 AI-Driven Vulnerability Discovery: The Linux Example

Linux runs most of the world’s servers, and its development is unusually transparent. That makes it a good indicator of what AI-assisted code analysis means for every large code base.

At the Linux Plumbers Conference 2026, engineers who maintain the kernel for a major cloud infrastructure presented two years of data. Before 2024 they saw about two kernel CVEs per week. Afterwards the rate rose to about sixteen per day, an increase of more than fifty times, and spikes of hundreds per day became common. On August 15, 2026, 848 kernel CVEs were published on a single day. Their conclusion was that manual triage is no longer possible. [Q01] Part of this growth is procedural, since the kernel project has assigned its own CVE identifiers since 2024 and states that it cannot judge which entries matter for a given system. [Q09] Trade reporting on data shared by the kernel’s stable maintainer adds the second cause: the number of CVEs fixed per kernel release rose from roughly 500 to more than 1,500 within a few releases, and most of the bugs in recent releases were found by AI code review platforms and large language models. [Q10]

The step from finding to exploiting has been automated as well. According to a report published on November 4, 2026, a prototype pipeline of one AI vendor identified 2,308 candidate vulnerabilities in the Linux kernel, reproduced 1,724 of them dynamically, and produced 948 distinct local privilege-escalation exploits that give an unprivileged user root access. The stated cost was about 1.2 million U.S. dollars in computing credits. The vendor expects that within a few years frontier models will likely discover whatever vulnerabilities exist in a given software project. [Q02] A second vendor reported in April 2026 that its unreleased model had found thousands of previously unknown, high-severity

© 2026 Beat W. Meier · All rights reserved.

Status: Public.

vulnerabilities, including some in every major operating system and every major web browser, and had autonomously chained several Linux kernel flaws into a complete takeover of a machine. [Q11]

Two caveats apply. Many kernel CVEs are of low severity or affect code that a given system does not use. [Q09], [Q10] And the vendors cited disclose their findings to maintainers so that they can be fixed. Neither caveat changes the structural point: the cost of finding an exploitable flaw in complex software is falling by orders of magnitude, and the capability will not remain with defenders alone. [Q11]

2.2 Recent Incidents in Switzerland and the United States

The danger is not hypothetical. The incidents of 2026 alone show the same pattern in both countries.

Switzerland. In the first half of 2026, the Federal Office for Cybersecurity received 27,128 voluntary reports and 200 reports of cyber incidents that are subject to mandatory reporting, and it counted 79 ransomware cases. The office adds that cyber sabotage has become a practicable instrument for individual states. [Q12]

The most serious case concerns the federal government itself. In late September 2026, attackers broke into PK Softech, a software supplier to pension funds, among them the federal pension fund Publica. According to trade reporting based on research by the Tages-Anzeiger, records of more than 100,000 current and former federal employees were taken, with names, dates of birth, social security numbers, addresses, and salary data, and in part bank details. The employer is visible even for staff of the federal police and the intelligence service who work under cover identities, and the federal government set up a task force. The attack is attributed to the ransomware group Akira. A city pension fund that had transferred data only to test a planned system change found that its members' data had been taken as well. [Q05]

Two further cases show the breadth. On April 30, 2026, the radiology network Groupe 3R, with 20 centers in western Switzerland, was attacked for the second time within a year. Company data were stolen and published by the perpetrators, medical data were encrypted and temporarily unusable, and the IT infrastructure of all centers had to be rebuilt. [Q13] In autumn 2026, data stolen from a security installation company in the canton of Vaud were offered for sale. According to the reporting, they include floor plans, camera positions, and in some cases access credentials for prisons, police facilities, banks, and companies. [Q14]

United States. The FBI's Internet Crime Complaint Center registered 1,008,597 complaints for 2025, with reported losses of 20.877 billion U.S. dollars, 26 percent more than in the year before. [Q07] In March 2026, attackers whom the U.S. government linked to an Iranian intelligence service broke into the medical technology manufacturer Stryker and remotely wiped tens of thousands of employee devices in a single stroke. Operations were disrupted for days, and the incident had a material impact on the company's quarterly earnings. In August 2026, a cyberattack cut off the global network of the medical device maker Boston Scientific. Orders and shipping stopped, and the immediate recovery took two weeks. In the education sector, attackers stole personal data of more than 30 million students and staff from the learning platform Canvas, later defaced its login pages during final examinations, and the operator eventually paid a ransom. [Q06]

Three observations follow. In nearly every case, the damage arose at a point of concentration: a supplier that held the data of many organizations, a central function from which tens of thousands of devices could be wiped at once, or a platform that stored the data of thousands of institutions. Data that had been handed over only for testing were lost together with production data. And the victims were not careless outsiders. They include the pension administration of a government and listed technology companies.

© 2026 Beat W. Meier · All rights reserved.

Status: Public.

2.3 Why Central Server Structures Concentrate the Risk

A flaw in software is dangerous in proportion to what the affected system holds. Central platforms hold everything: the accounts of all users, their content or at least its ciphertext, keys or key-recovery material, and the metadata of every interaction. A single successful attack therefore scales to the whole user base.

Two official investigations illustrate this. The U.S. Cyber Safety Review Board examined the 2023 intrusion into a major cloud mail service. One compromised signing key allowed the attackers to access the mailboxes of 22 organizations and more than 500 individuals, and the Board concluded that the intrusion was preventable. [Q15] In November 2024, the FBI and CISA confirmed that state-affiliated actors had compromised the networks of several telecommunications companies. The attackers stole customer call records, intercepted private communications of selected individuals, and copied information that was subject to law enforcement requests under court orders. [Q16] The second case deserves attention because the access facilities that operators must maintain for authorities became a target themselves.

AI-driven vulnerability discovery multiplies this exposure. A central service must patch every relevant flaw before any attacker uses it, across a stack of operating system, virtualization, and application software that changes daily. Section 2.1 shows that this race is becoming harder to win.

2.4 Quantum Computing and Harvest Now, Decrypt Later

Today’s key exchange and digital signatures rely on mathematical problems that a sufficiently large quantum computer could solve. NIST finalized its transition report in October 2026. It will deprecate quantum-vulnerable public-key cryptography, including RSA, Diffie-Hellman, and elliptic-curve methods, after 2030 and disallow it under its standards after 2035. The report names the reason for urgency: in the threat known as harvest now, decrypt later, adversaries collect encrypted data today in order to decrypt it once the technology matures. Symmetric cryptography is considerably less affected. [Q03] The replacement standards exist. NIST published its first post-quantum key-encapsulation standard in August 2024. [Q17]

How far away is the threat? Estimates keep moving in one direction. In 2019, factoring a 2048-bit RSA key was estimated to require 20 million noisy qubits. A 2025 analysis by a researcher at a leading quantum laboratory reduces this to fewer than one million noisy qubits and less than a week of runtime, under unchanged hardware assumptions. [Q18] No such machine exists today. But data that must stay confidential for ten or twenty years is already exposed if its ciphertext can be recorded now.

This shifts attention to a question that is easy to overlook: where can ciphertext be collected in bulk? The answer is, again, at central points, such as platforms that store encrypted archives for millions of users and network locations where their traffic converges.

© 2026 Beat W. Meier · All rights reserved.

Status: Public.

2.5 Lawful Access and Jurisdiction

The second challenge is not an attack but a legal design. Section 2713 of Title 18 of the United States Code, added by the CLOUD Act in 2018, requires providers of communication and cloud services to preserve and disclose data in their possession, custody, or control, regardless of whether the data are located within or outside the United States. [Q04] The decisive criterion is thus control by a provider under U.S. jurisdiction, not the location of the data center. A European or Swiss data center operated by such a provider does not change the legal reach.

The United States is not the only example. Swiss law obliges telecommunications providers to retain connection data and to support surveillance measures. [Q19] In the United Kingdom, a leading device manufacturer announced in 2025 that it could no longer offer its end-to-end encrypted cloud storage option to new users there, while stating that it had never built a backdoor into its products. [Q20] This study does not assess the legitimacy of such powers. They exist in democratic states under judicial procedures. The architectural observation is narrower: every one of these instruments addresses an intermediary who holds data or keys. Where no intermediary holds readable data, an order can only be directed at the people who actually communicate. That is where the rule of law traditionally places it.

For industry, public authorities, and private individuals alike, the consequence is a dependency that contracts cannot remove. As long as a third party can technically read or hand over the data, the confidentiality of that data depends on the legal order and the internal security of that third party.

2.6 Synthesis

Pressure	What changes	Why central platforms are exposed
AI-driven vulnerability discovery	Exploitable flaws are found and weaponized faster and at lower cost	One flaw in one platform exposes all users and all data at once
Quantum computing	Recorded ciphertext may become readable later	Platforms and their network edges are the natural collection points for ciphertext in bulk
Lawful access across borders	Providers must disclose what they control, regardless of location	The platform operator is the addressee who holds data, keys, or metadata
Insider and operator risk	Administrators and suppliers have technical access	Concentrated privileges allow concentrated misuse

All four pressures act on the same structural property. The following principles therefore do not start with stronger walls around the center. They start by asking which functions need a center at all.

3. Design Principles of the Response

3.1 No Central Point That Holds Identities, Content, and Keys

The first principle is separation. Central services combine identity, content protection, transport, intermediate storage, and billing in one hand. If these functions are separated and assigned to different parties that cannot combine their knowledge, the compromise of one party no longer reveals the whole. Identities are created on the device and are not registered anywhere. Billing and operating permits are handled by an administration that never sees communication data.

3.2 End-to-End Encryption with Keys Only on End Devices

Content is encrypted on the sending device and decrypted on the receiving device. The methods for this are published and formally analyzed. The Double Ratchet algorithm renews keys continuously, so that a compromised key reveals neither earlier nor, after recovery, later messages. [Q21], [Q22] Research regards content protection among leading messengers as largely solved, while the protection

© 2026 Beat W. Meier · All rights reserved.

Status: Public.

of metadata remains open. [Q23] The principle here extends the same rule to everything stored: data at rest on the device is encrypted with a secret that only the user holds and that no provider can reset.

3.3 Transport over an Anonymized Network

Encryption hides what is said, not who speaks with whom. The second layer therefore routes all traffic through an anonymized network in which several independent stations relay the data in layered encryption, a concept that goes back to Chaum's work on untraceable communication. [Q08] No station knows both ends of a connection, and neither the service nodes nor an observer of the user's access line learn the user's counterpart. Where this principle is applied strictly, there is no fallback: if the anonymized network is unavailable, protected traffic stops and never takes a direct route.

The research literature is clear about the limits. Strong anonymity, low latency, and low bandwidth overhead cannot all be achieved at once. [Q24] A low-latency anonymized network does not protect against an adversary who can observe both ends of a connection at the same time.

3.4 Segmented Data Storage

Data stores of the future are segmented. Not all data are kept in one place in one system. This principle answers all four pressures of Section 2.6 at once, and it has three dimensions.

Segmentation by function means that the party who stores a message cannot identify its participants, and the party who admits a node or bills a license never sees a message. Segmentation by owner means that data belong to the smallest sensible unit, the device of a person or the infrastructure of one organization, and are not pooled across customers on a shared platform. Segmentation by location means that data that must be stored outside a device are split into encrypted copies on several independent storage nodes, chosen at random and replaced over time, so that no node has a complete or lasting picture.

The idea follows the classic security principles of least privilege and separation of privilege, formulated by Saltzer and Schroeder in 1975. [Q25] Its effect is that a successful attack, a recorded ciphertext stream, or a disclosure order yields a fragment and not the whole.

3.5 Private-by-Default Reachability

A server that cannot be reached cannot be attacked from the internet at large. Where servers are needed, they are not exposed publicly and are reachable only through an encrypted private mesh whose members are admitted individually. This corresponds to the zero-trust model standardized by NIST, in which access is granted per device and per request and never on the basis of network location. [Q26] Against automated mass exploitation as described in Section 2.1, removing the public attack surface is one of the most effective measures available.

© 2026 Beat W. Meier · All rights reserved.

Status: Public.

3.6 Memory-Safe Implementation and a Small Attack Surface

A large share of exploitable flaws in system software are memory-safety errors. Government cybersecurity agencies of several countries therefore urge manufacturers to move to memory-safe programming languages. [Q27] Both demonstrators implement their security-relevant core in such a language, use one shared core on all platforms, and rely on established, published cryptographic building blocks without cryptography of their own invention. Functions that are not needed are not built in. There is no telemetry and there are no advertising or analytics components.

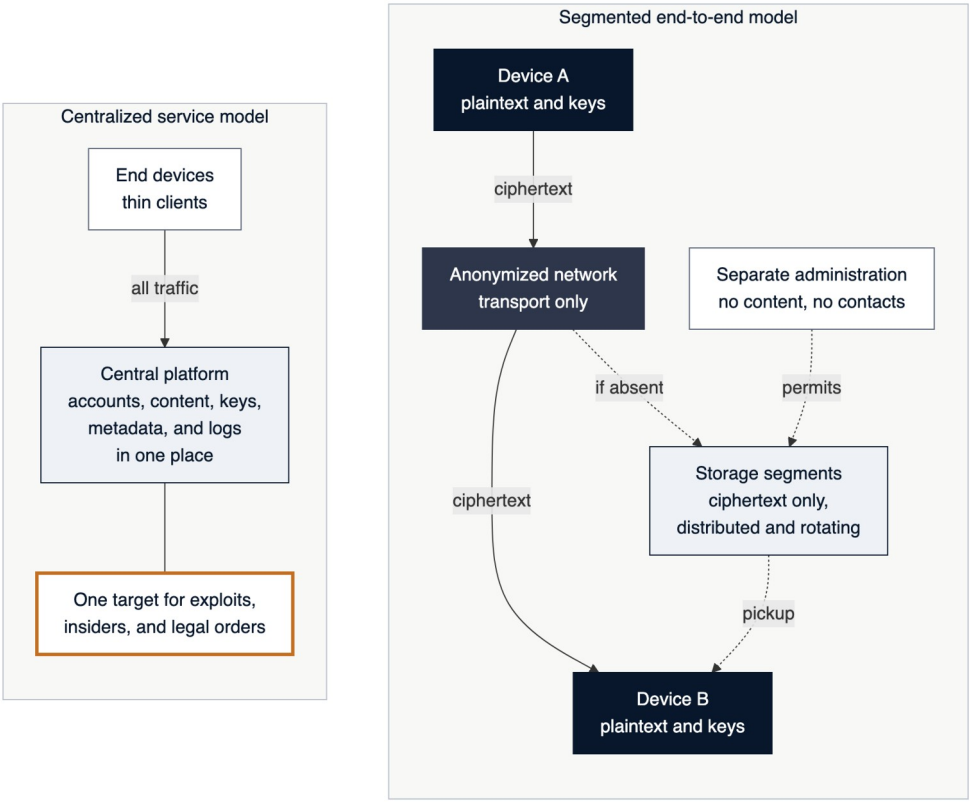


Figure 1: Centralized service model and segmented end-to-end model.

In the centralized model, one platform holds accounts, content, keys, and metadata and is therefore a single target. In the segmented model, plaintext and keys exist only on end devices, the anonymized network only transports, storage nodes hold distributed ciphertext, and a separate administration receives no communication data. Author's illustration, without protocol details.

4. Technology Demonstrator 1: HeyAppPro

4.1 Purpose

HeyAppPro is a messenger for people and organizations who want confidential communication without depending on a single provider's servers and data access. It covers text messages, media and file attachments, and voice communication. Its design assumption is strict: a cloud or platform provider, or an authority, obtains all data stored at any provider. Without a secret held exclusively by the user, these data must allow neither the decryption of conversations nor the takeover of an identity.

© 2026 Beat W. Meier · All rights reserved.

Status: Public.

4.2 Principle of Operation

Identity without a registry. A person's identity is a cryptographic pseudonym generated on the device. No phone number or e-mail address is required, and no central directory records who uses the system. Contacts are established through single-use invitations with a limited lifetime, passed on as a link or a QR code, and can be verified by the two people involved.

Content protection. Messages and attachments are encrypted end to end with an established ratchet method. [Q21] Keys never leave the devices. All local data are encrypted and can be opened only with a separate app password that is neither stored permanently nor transmitted, and that no provider can reset. Keys and conversations are excluded from automatic cloud backups.

Transport. All communication runs exclusively over the anonymized network. An app-level kill switch blocks protected traffic whenever this transport is unavailable, at startup, after a failure, and during a network change. A direct connection is never used as a fallback.

Delivery to absent recipients. Phones and laptops are not always online. Central messengers solve this with a queue at the operator. HeyAppPro instead deposits the fully encrypted message with a small group of randomly selected, continuously available nodes assigned to the contact relationship. The membership of this group is renewed over time, autonomously and without the participation of the end devices, which may both be offline. A private index, itself stored redundantly and unreadable to outsiders, allows the recipient to find the copies even if the sender has since switched off. Only the recipient's authenticated receipt triggers the deletion of all copies.

Separated administration. A node may serve the network only with a short-lived operating permit issued by a separate authority. This authority can exclude faulty or hostile nodes, and it never receives message content, contact lists, or identities of people. Licensing and payment are separated from communication in the same way.

Closed networks for organizations. An organization can operate its own closed network within the same architecture, with nodes it admits itself, signed administrative actions, four-eyes approval for critical steps, and a tamper-evident audit record.

© 2026 Beat W. Meier · All rights reserved.

Status: Public.

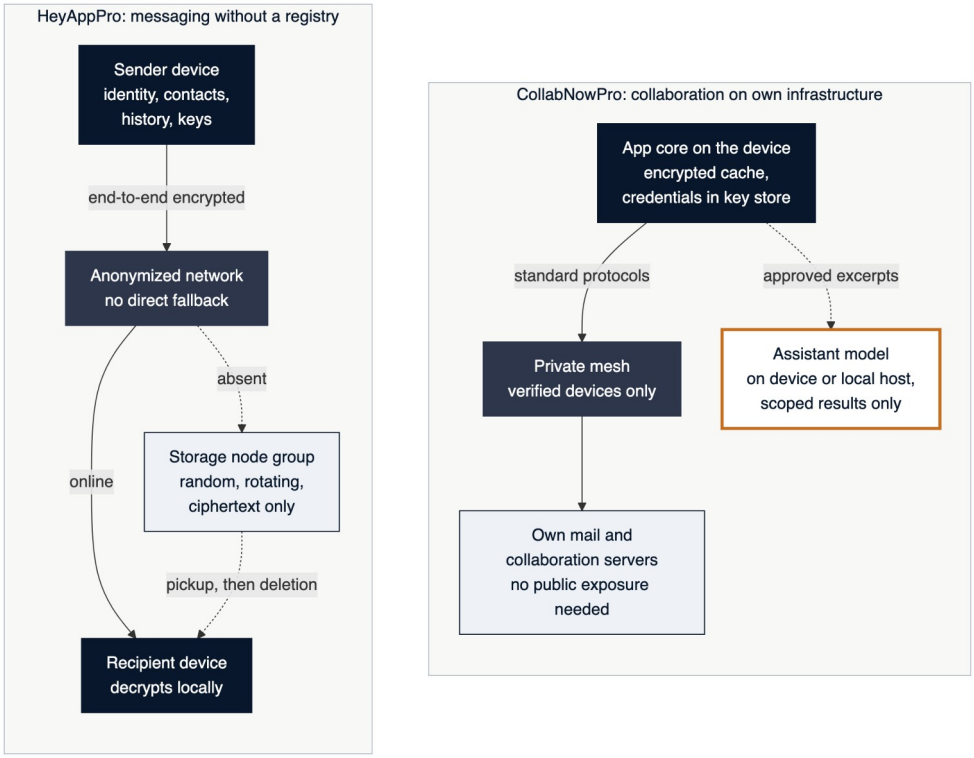


Figure 2: Principle of operation of the two technology demonstrators.

HeyAppPro transports end-to-end encrypted messages over the anonymized network and stores them for absent recipients as ciphertext on a rotating group of nodes. CollabNowPro connects an application core on the device through a private mesh with mail and collaboration servers that the organization itself controls, and it confines the AI assistant to approved excerpts. Author's illustration, without protocol details.

4.3 Advantages

- **No central target.** There is no subscriber registry, no central message store, and no central log of who communicates with whom. An attacker who compromises a node obtains ciphertext fragments without knowledge of the people behind them.
- **Reduced value of disclosure orders against intermediaries.** No operator or node holds readable content, contact lists, or content keys. What does not exist at an intermediary cannot be handed over by it.
- **Protection of metadata.** Neither the nodes nor an observer of the user's access line learn the network address of the counterpart. Identities are not tied to phone numbers.
- **Segmented storage.** Stored messages exist only as encrypted copies on several independent nodes that change over time, and they are deleted after confirmed delivery.
- **Reliable delivery without a central queue.** Messages reach recipients who were offline, even if the sender has gone offline in the meantime.
- **Control over the device.** Local data remain encrypted, and the app locks itself when it moves to the background. Automatic deletion of conversations after a short retention period is specified as a further requirement.
- **Governable operation.** The operating authority can stop individual nodes or an entire network without gaining any ability to read or delete user data.
- **One memory-safe core on all platforms.** The same core serves desktop and mobile systems, which shortens the code that must be audited.

© 2026 Beat W. Meier · All rights reserved.

Status: Public.

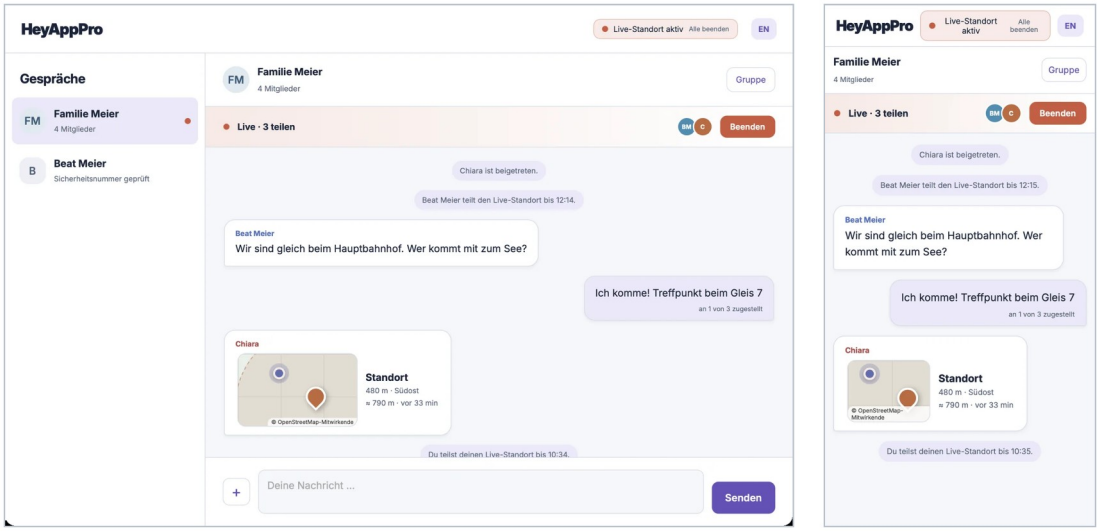


Figure 3: HeyAppPro on the desktop and on a phone.

The group conversation shows the delivery status of a message and a shared live location. Captures of the application interface in German with sample data.

4.4 Implementation Status and Evidence

According to the project's progress records, the following has been demonstrated. Messages are exchanged over the anonymized network between desktop and mobile devices. A live test fleet of nodes on several independent hosts is in operation, and on November 8, 2026 a physical tablet was connected to all nodes of this fleet. Automatic issuance, use, revocation, and expiry of admission policies were verified in a separate test over the real anonymized network. A fleet simulation with 99 clients that exchange texts, images, and positions, switch off and on according to plan, and verify every delivery has been implemented as a development tool. The project's automated test suites passed at the last recorded run on November 10, 2026. Builds exist for macOS, iOS, Android, Windows, and Linux.

The following is implemented and tested locally but not yet accepted in live operation: closed customer networks with signed administration, and the related licensing. Still outstanding are complete acceptance on physical Android devices, signed and reproducible releases for all platforms, long-term operation of the autonomous node renewal at scale, and an independent security audit. The project's own documents state that no milestone has been formally accepted as a product.

5. Technology Demonstrator 2: CollabNowPro

5.1 Purpose

Messaging is one part of digital work. The larger part consists of mail, calendars, contacts, tasks, notes, and files, today typically consumed as a suite from a hyperscale cloud provider. CollabNowPro unites these functions and an AI assistant in a single application for mobile devices and the desktop, and it works against infrastructure the organization itself controls. An account with a cloud suite provider is not required. An existing corporate groupware system can be connected as an additional account where an organization still depends on it.

© 2026 Beat W. Meier · All rights reserved.

Status: Public.

5.2 Principle of Operation

One core, open protocols. A single application core, written in a memory-safe language, contains the logic for mail, calendar, contacts, tasks, notes, files, search, and reminders. It speaks the open standard protocols for these functions, so the data remain in formats and on servers the organization can move at any time. The user interfaces for phone, tablet, and desktop are thin layers above this core.

Private mesh. In the reference setup, the application reaches the organization's mail and collaboration servers only through an encrypted private mesh to which each device is admitted individually. The servers therefore need not be exposed to the public internet. When this mode is active, the application requires a verified mesh connection and never falls back to a direct route.

Protection on the device. The device keeps only an encrypted cache of recently used data for offline work. Account credentials are stored in the protected key store of the operating system. Changes made offline are marked as pending and are transmitted later with version checks, and an action counts as done only after the server has confirmed it.

An assistant under the application's control. The assistant can read, summarize, and prepare actions across all functions in a chat, and the design also provides for voice. The decisive design choice is where control lies. The application, not the model, performs data access and actions. The model receives only the excerpts approved for the task and never the account credentials. Users define areas that determine which calendars, address books, mail folders, and lists the assistant may read or change. Every change appears as a card for confirmation. The model runs on the device or on hardware in the organization's own possession. An external model service is used only if the user selects one explicitly, and an automatic fallback to a cloud model does not exist.

5.3 Advantages

- **Data stay under the organization's own jurisdiction.** No third-party platform stores or processes the content. The question of which foreign statute applies to the provider does not arise, because there is no such provider in the path.
- **No public attack surface.** Servers that are reachable only through the private mesh are out of reach for automated mass scanning and exploitation.
- **Segmentation by owner.** Each organization's data remain in its own systems and are not pooled with those of other customers on a shared platform. A flaw in one installation does not expose another.
- **AI assistance without data outflow.** With the model on the device or on local hardware, sensitive content is not sent to an external AI service, and the assistant acts only within areas the user has approved.
- **One application in place of many.** Mail, appointments, tasks, contacts, notes, and files share one search and one overview. The assistant turns recurring multi-step work into a single confirmed instruction.
- **No lock-in.** Open protocols and self-operated servers keep the organization free to change components.
- **Full manual control.** Everything remains directly usable without the assistant.

© 2026 Beat W. Meier · All rights reserved.

Status: Public.

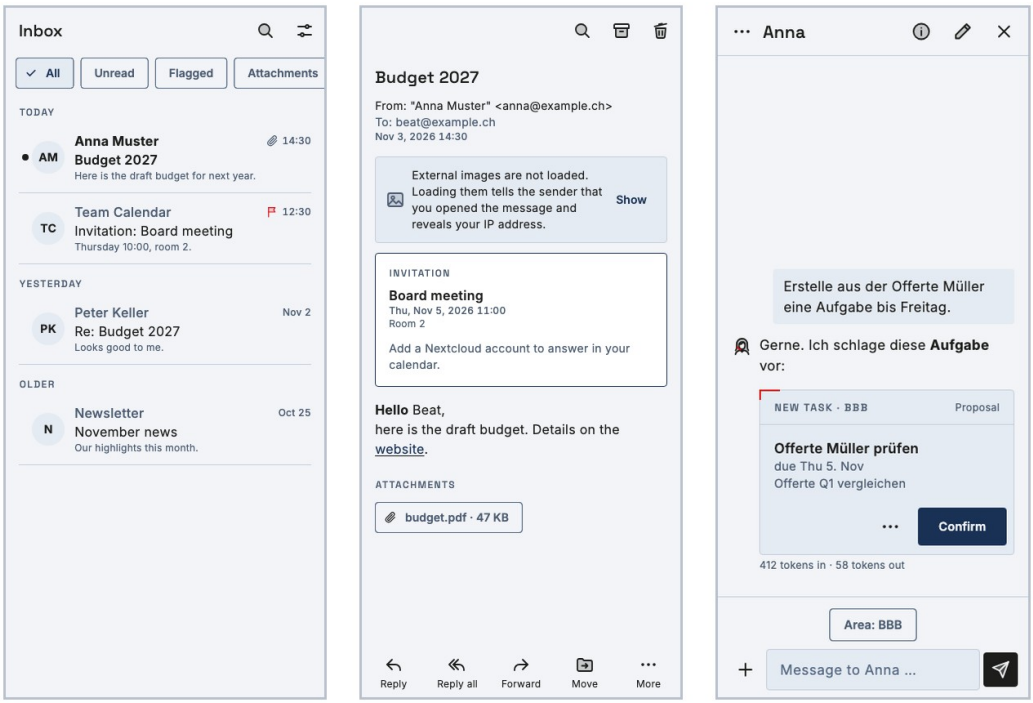


Figure 4: CollabNowPro on a phone.

From left to right: the inbox, a message with blocked external images and a meeting invitation, and the assistant proposing a task as a card that the user confirms. Captures of the application interface from the project's test suite with invented sample data.

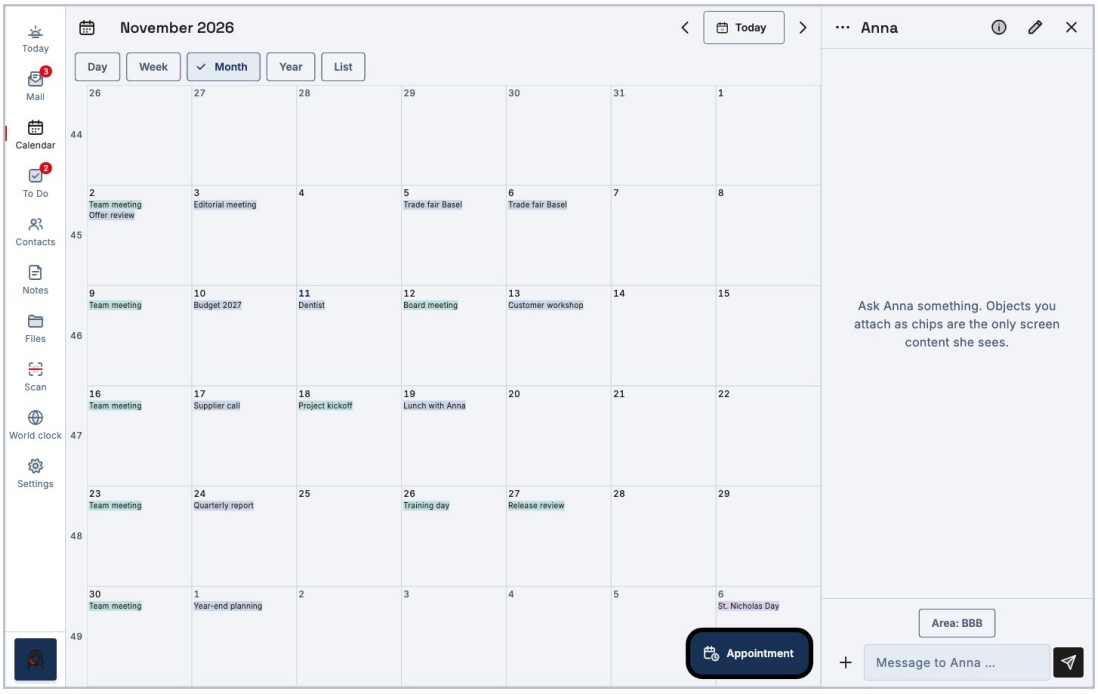


Figure 5: CollabNowPro on the desktop.

The calendar in the month view, with the navigation bar on the left and the assistant as a sidebar on the right, where the only screen content it sees are the objects the user attaches. Capture of the application interface in the wide layout, rendered with the project's test tooling and invented sample data.

© 2026 Beat W. Meier · All rights reserved.

Status: Public.

5.4 Implementation Status and Evidence

The desktop application exists with a broad, tested range of mail, calendar, contact, task, note, and file functions. The mobile application has been running on a physical tablet connected through the private mesh to the organization’s servers since November 10, 2026. Device tests on November 11, 2026 confirmed, each with verification on the server, the reading and handling of mail, calendar views and entries, and the creation, change, and deletion of tasks, contacts, notes, and folders. The last recorded run of the automated tests of the core passed without failures. Tests that require the live server environment are kept separately.

Open points recorded by the project include slow global search and contact loading on the tablet, the handling of an outgoing message whose delivery state is unknown, complete acceptance on Android devices, release hardening, and an independent security review.

5.5 Sealed Mail

One function joins the two demonstrators. Both applications offer an option to send e-mail in sealed form. A sealed message is encrypted end to end on the basis of the OpenPGP standard. [Q28] Keys are generated and managed automatically in the background and are exchanged only between correspondents, without publication in any directory. Sealed messages travel exclusively over the anonymized network through nodes of the existing fleet. These nodes hold each message for a random time and change its apparent size, so that even large-scale statistical observation finds it difficult to match what enters with what leaves. A confirmation of receipt returns by the same path and appears to the sender as a check mark. The user sees none of this machinery, only the option to send securely and the confirmation of receipt. A message marked for sealed delivery is never sent unencrypted without the sender’s explicit decision.

The principle behind the design is the mix concept described by Chaum. [Q08] Its limits are those named in Section 3.3, and the design itself excludes claims of absolute anonymity.

6. Discussion

6.1 How the Demonstrators Answer the Four Pressures

Pressure	HeyAppPro	CollabNowPro
AI-driven vulnerability discovery	No central system whose compromise exposes all users; nodes hold only ciphertext fragments; memory-safe core	Servers need no public exposure; one installation per organization; memory-safe core; credentials only in the device key store
Quantum computing	Fewer points where ciphertext accumulates; stored copies are distributed and deleted after delivery; post-quantum algorithms not yet in use	No ciphertext archive at a third party; mesh traffic stays between own devices and own servers; post-quantum algorithms not yet in use
Lawful access across borders	No intermediary holds readable content, contact lists, or a subscriber registry	No third-party provider in the path; data stay with the organization, under its own jurisdiction
Insider and operator risk	Administration separated from communication; signed actions, four-eyes approval, audit record	Assistant confined to approved areas and excerpts; each change requires confirmation

© 2026 Beat W. Meier · All rights reserved.

Status: Public.

6.2 Residual Risks and Limits

Quantum resistance has not been achieved. Neither demonstrator currently uses post-quantum algorithms for key agreement or signatures, and the anonymized network itself relies on classical public-key methods. The architecture reduces how much ciphertext an adversary can collect at any one point, which lowers the yield of harvest now, decrypt later. It does not remove the threat. Sealed mail is based on a standard whose common key types are also quantum-vulnerable. Migration to the standardized post-quantum methods within the schedule set by NIST is therefore necessary. [Q03], [Q17]

Anonymity is not absolute. An adversary who observes both ends of a connection, or large parts of the network over a long time, can correlate traffic. [Q24] With few users, the set of people among whom a user is hidden is small. Sizes and times remain visible in coarse form to the nodes involved.

Segmented storage has a fault model. Replication across a small group of nodes survives the failure of individual nodes. It does not survive a malicious majority, which would require Byzantine fault-tolerant protocols with more replicas. [Q29] Open participation would additionally invite attackers to operate many nodes under false identities. [Q30] HeyAppPro counters this with the admission of nodes by a central authority.

The central operating authority is a deliberate dependency. It solves the admission problem and at the same time creates a dependency for availability and trust. It cannot read messages, but it can stop the network.

CollabNowPro relies on servers. The architecture moves the servers out of public reach and into the organization’s own hands. It does not eliminate them. Within one organization, collaboration data remain concentrated on its own systems, and the organization bears the operational duty that a cloud provider would otherwise assume. Ordinary e-mail to outside recipients continues to pass through their providers in the usual way.

End devices remain decisive. If a device is compromised or its operating system manipulated, decrypted content can be captured there. Screenshots, weak passwords, and the recipient’s device are outside the control of either application. Mobile operating systems also limit background activity, which can delay delivery.

Assurance is still pending. Both demonstrators are working software, but neither has passed an independent security audit, and device acceptance is incomplete. Their protection claims are design properties supported by the project’s own tests, not certified guarantees.

6.3 Counter-Positions

The case for central platforms is not weak, and it should be stated. Large providers employ security teams and patch at a speed that small organizations cannot match. The very AI systems that find vulnerabilities are being given to defenders first, with the explicit aim of fixing critical software before attackers can use the same capability. [Q11] Self-operated infrastructure that is neglected can be less secure than a professionally run cloud. Decentralization also costs usability and performance: an anonymized network is slower than a direct connection, and a user who loses the only secret loses access to the data, because no provider can reset it.

These objections do not refute the argument. They define its scope. The architecture described here does not rest on the assumption that its own software will be free of flaws. It rests on limiting what a flaw, a recorded data stream, or an order can reveal. For communication whose confidentiality must

© 2026 Beat W. Meier · All rights reserved.

Status: Public.

hold for many years and against capable adversaries, limiting the damage is the more robust strategy. For data of low sensitivity, the convenience of central services may well prevail.

7. Conclusion and Recommendations

AI-driven vulnerability discovery, the foreseeable end of today's public-key cryptography, and cross-border access rights are independent developments that converge on the same structural weakness, the central platform that holds identities, content, keys, and metadata in one place. Hardening this platform further treats the symptom. The alternative is an architecture that does not require it: end-to-end encryption with keys only on end devices, transport over an anonymized network, segmented data storage, servers that are not publicly reachable, and a small, memory-safe code base.

HeyAppPro and CollabNowPro demonstrate that this alternative can be built with today's means and used on ordinary devices. HeyAppPro shows it for person-to-person communication without any subscriber registry. CollabNowPro shows it for the daily work of an organization, including AI assistance that does not send data to third parties. Both prove feasibility. Product maturity remains to be shown.

Five recommendations follow from the analysis.

1. **Commission independent security audits** of both demonstrators, including the anonymized transport, the storage and renewal mechanisms, and the administrative functions, and publish the results in suitable form.
2. **Plan the post-quantum migration now.** Introduce standardized post-quantum key establishment in hybrid form first for content protection and long-lived stored data, and design all protocols so that algorithms can be exchanged.
3. **Complete device and live acceptance**, in particular on physical Android devices, for closed customer networks in live operation, and for long-term autonomous renewal of storage groups under load.
4. **Extend segmentation in CollabNowPro.** Examine how collaboration data within one organization can be divided further, so that the compromise of a single server reveals less.
5. **Communicate the limits as clearly as the advantages.** Protection goals, the adversary model, and residual risks belong in every product description. Absolute promises of anonymity or security should be avoided.

References

Online sources were accessed on November 11, 2026, unless noted otherwise. Sources [Q04], [Q19], [Q21], [Q22], [Q23], [Q29], and [Q30] were last accessed on October 19 or 20, 2026. Vendor publications are self-disclosures.

[Q01] Johnson, D.; Bouron, J.; Zielman, A.; Kudrjavets, G. Kernel CVEs at AWS Scale: Two Years of Empirical Findings. Linux Plumbers Conference 2026, Prague, presentation slides. https://lpc.events/event/20/contributions/2373/

[Q02] Larabel, M. OpenAI Finds 948 Local Privilege Escalation Bugs In The Linux Kernel. Phoronix, November 5, 2026. Trade report on OpenAI, A thousand fewer paths to root, November 4, 2026; the original publication could not be retrieved by automated access on November 11, 2026. https://www.phoronix.com/news/OpenAI-948-Linux-LPE-Bugs

[Q03] Moody, D.; Perlner, R.; Regenscheid, A.; Robinson, A.; Cooper, D. Transition to Post-Quantum Cryptography Standards. NIST Internal Report 8547, final, October 2026. https://doi.org/10.6028/NIST.IR.8547

[Q04] United States Code. 18 U.S.C. § 2713, Required preservation and disclosure of communications and records, added by Pub. L. 115-141 (CLOUD Act), March 23, 2018. https://uscode.house.gov/us/usc/119-118/t18/s2713/

© 2026 Beat W. Meier · All rights reserved.

Status: Public.

[Q05] Netzwoche. Update: Zürcher Pensionskasse verschiebt Softwareumstellung nach Cyberangriff. Running coverage of the data leak at PK Softech and Publica, with reference to the Tages-Anzeiger, first published October 8, 2026, updated November 4, 2026. https://www.netzwoche.ch/news/2026-10-08/bundespensionskasse-publica-meldet-datenabfluss

[Q06] TechCrunch. Leaks, data breaches, and ransom notes: The worst hacks of 2026 so far. First published June 8, 2026, updated September 15, 2026. https://techcrunch.com/2026/09/15/the-worst-hacks-and-breaches-of-2026-so-far/

[Q07] Federal Bureau of Investigation, Internet Crime Complaint Center. Internet Crime Report 2025. 2026. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[Q08] Chaum, D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24(2), 1981. https://doi.org/10.1145/358549.358563

[Q09] The Linux Kernel Organization. CVEs. The Linux Kernel documentation, process guide. https://www.kernel.org/doc/html/latest/process/cve.html

[Q10] TechSpot. AI is finding thousands of bugs in Linux, and maintainers can barely keep up. September 2026. Trade report on data published by the Linux stable kernel maintainer. https://www.techspot.com/news/113716-ai-finds-1500-vulnerabilities-linux-kernel-linus-torvalds.html

[Q11] Anthropic. Project Glasswing. April 7, 2026. https://www.anthropic.com/glasswing

[Q12] Federal Office for Cybersecurity (BACS). Halbjahresbericht 2026/1. Swiss Confederation, published August 24, 2026. https://www.bacs.admin.ch/de/hjb-26-de1

[Q13] Netzwoche. Update: Westschweizer Radiologienetzwerk bestätigt Datendiebstahl nach Cyberangriff. May 7, 2026, updated July 7, 2026. https://www.netzwoche.ch/news/2026-05-07/cyberangriff-legt-westschweizer-radiologie-netzwerk-erneut-lahm

[Q14] Netzwoche. Cyberangriff auf Waadtländer Firma legt sensible Sicherheitsdaten offen. October 8, 2026, with reference to Le Temps. https://www.netzwoche.ch/news/2026-10-08/cyberangriff-auf-waadtlaender-firma-legt-sensible-sicherheitsdaten-offen

[Q15] Cyber Safety Review Board. Review of the Summer 2023 Microsoft Exchange Online Intrusion. U.S. Department of Homeland Security, released April 2, 2024. https://www.cisa.gov/resources-tools/resources/CSRB-Review-Summer-2023-MEO-Intrusion

[Q16] Federal Bureau of Investigation; Cybersecurity and Infrastructure Security Agency. Joint Statement from FBI and CISA on the People's Republic of China (PRC) Targeting of Commercial Telecommunications Infrastructure. November 13, 2024. https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications

[Q17] National Institute of Standards and Technology. Module-Lattice-Based Key-Encapsulation Mechanism Standard. FIPS 203, August 13, 2024. https://doi.org/10.6028/NIST.FIPS.203

[Q18] Gidney, C. How to factor 2048 bit RSA integers with less than a million noisy qubits. arXiv:2505.15917, May 21, 2025. https://arxiv.org/abs/2505.15917

[Q19] Swiss Confederation. Federal Act on the Surveillance of Post and Telecommunications (BÜPF/SPTA) of March 18, 2016, SR 780.1, status as of September 1, 2023; official German text. https://www.fedlex.admin.ch/eli/cc/2018/31/de

[Q20] Apple. Apple can no longer offer Advanced Data Protection in the United Kingdom to new users. Apple Support. https://support.apple.com/en-us/122234

[Q21] Perrin, T.; Marlinspike, M.; Schmidt, R. The Double Ratchet Algorithm. Signal Specifications, Revision 4, November 4, 2025. https://signal.org/docs/specifications/doubleratchet/

[Q22] Cohn-Gordon, K.; Cremers, C.; Dowling, B.; Garratt, L.; Stebila, D. A Formal Security Analysis of the Signal Messaging Protocol. Journal of Cryptology 33, 2020. https://doi.org/10.1007/s00145-020-09360-1

[Q23] Unger, N.; Dechand, S.; Bonneau, J.; Fahl, S.; Perl, H.; Goldberg, I.; Smith, M. SoK: Secure Messaging. IEEE Symposium on Security and Privacy, 2015. https://doi.org/10.1109/SP.2015.22

[Q24] Das, D.; Meiser, S.; Mohammadi, E.; Kate, A. Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency, Choose Two. IEEE Symposium on Security and Privacy, 2018. https://doi.org/10.1109/SP.2018.00011

[Q25] Saltzer, J. H.; Schroeder, M. D. The Protection of Information in Computer Systems. Proceedings of the IEEE 63(9), 1975. https://doi.org/10.1109/PROC.1975.9939

[Q26] Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. Zero Trust Architecture. NIST Special Publication 800-207, August 2020. https://doi.org/10.6028/NIST.SP.800-207

[Q27] Cybersecurity and Infrastructure Security Agency; National Security Agency; Federal Bureau of Investigation; international partner agencies. The Case for Memory Safe Roadmaps. December 2023. https://www.cisa.gov/resources-tools/resources/case-memory-safe-roadmaps

[Q28] Wouters, P. (ed.); Huigens, D.; Winter, J.; Niibe, Y. RFC 9580: OpenPGP. IETF, July 2024. https://www.rfc-editor.org/rfc/rfc9580.html

[Q29] Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance. 3rd Symposium on Operating Systems Design and Implementation (OSDI), 1999. https://www.usenix.org/conference/osdi-99/practical-byzantine-fault-tolerance

[Q30] Douceur, J. R. The Sybil Attack. Peer-to-Peer Systems, IPTPS 2002, Lecture Notes in Computer Science 2429. https://doi.org/10.1007/3-540-45748-8_24

© 2026 Beat W. Meier · All rights reserved.

Status: Public.