Group Messaging in The Guardian's Anonymous Whistleblowing System

CedarCrypt 2026, Paphos

Zeke Hunter-Green

@zekehg.bsky.social

Daniel Hugenroth

@lambda.bsky.social

The Guardian

UNIVERSITY OF CAMBRIDGE

The CoverDrop team

The original CoverDrop research team


Mansoor Ahmed


Daniel Hugenroth


Diana A. Vasile


Alastair R. Beresford


Ross Anderson

The Guardian crew and contributors


Sam Cutler


Luke Hoyland

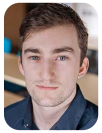

Philip McMahon


Tom Richards


Zeke Hunter-Green


Sabina Bejasa-Dimmock


Marjan Kalanaki


Sam Hession


Dom Kendrick


Mario Savarese


Chloe Kirton

UNIVERSITY OF CAMBRIDGE
Department of Computer Science and Technology

The Guardian

NOKIA BELL LABS

OPEN TECHNOLOGY FUND

Imagine you have discovered wrongdoings and are ready to talk a journalist…

how would you do that?

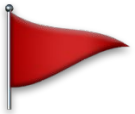
The **first contact** is particularly difficult

The **first contact** is
particularly difficult

Avoid leaving **digital footprints**
from the beginning

The **first contact** is
particularly difficult

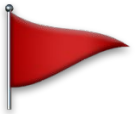
Avoid leaving **digital footprints**
from the beginning



Using anonymity networks (e.g. Tor)
can make one **stand-out**…

The **first contact** is
particularly difficult

Avoid leaving **digital footprints**
from the beginning



Using anonymity networks (e.g. Tor)
can make one **stand-out**…

…and they can be
difficult to use

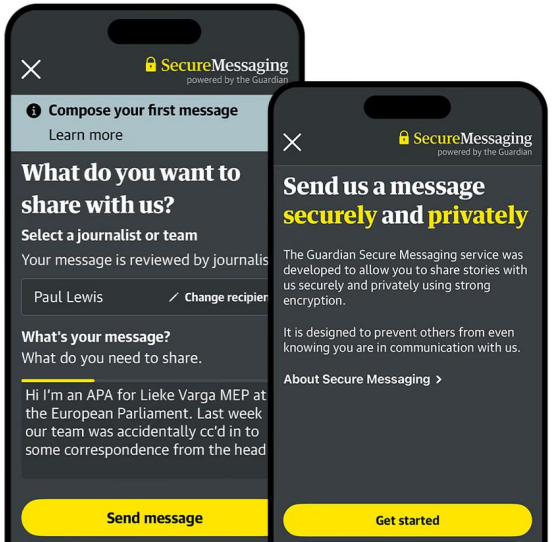
Blowing the whistle is impactful, but tricky.

Blowing the whistle is impactful, but tricky.

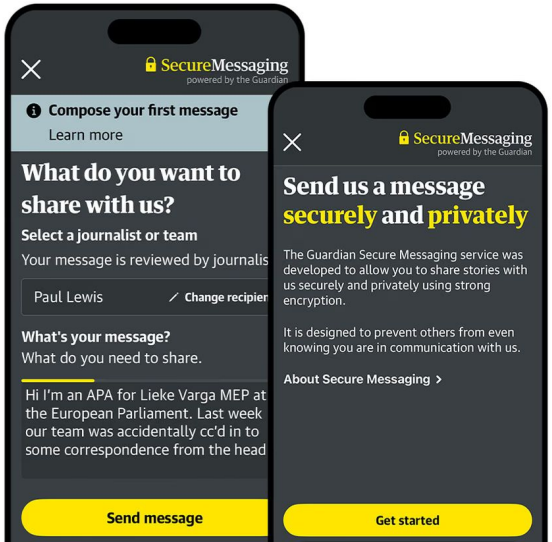
Blowing the whistle is impactful, but tricky.

Blowing the whistle is impactful, but tricky.

Secure Messaging

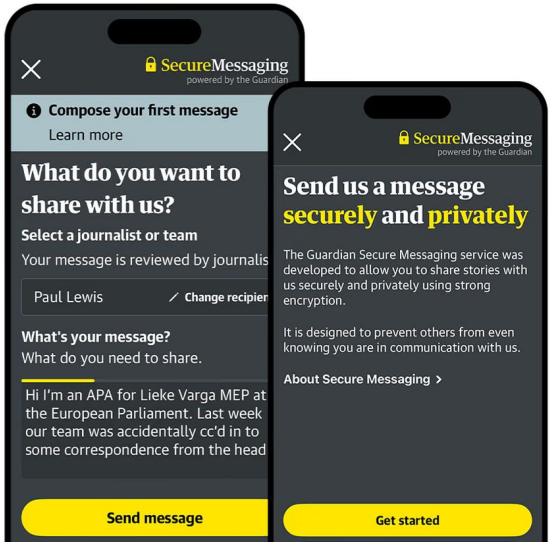


Secure Messaging



Embedded and activated in every Guardian app

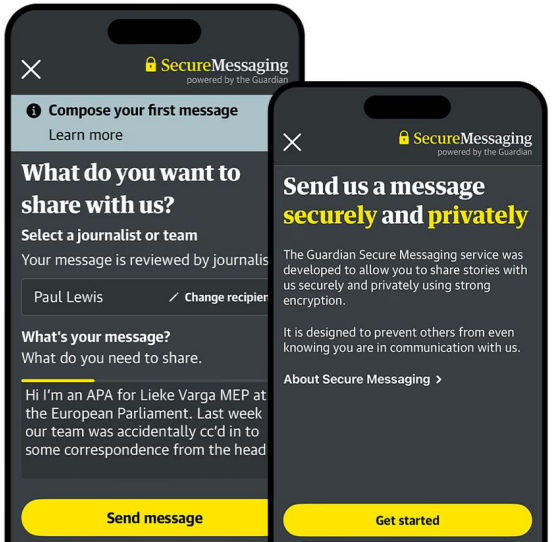
Secure Messaging



Embedded and activated
in every Guardian app

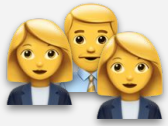
Cover traffic protects metadata of
real whistleblower messages

Secure Messaging



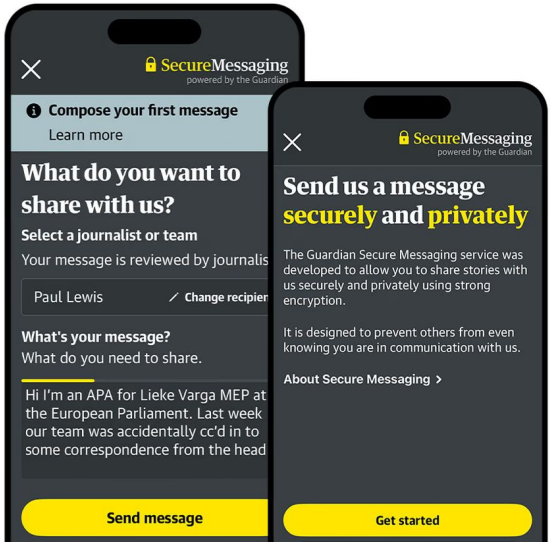
Embedded and activated in every Guardian app

Cover traffic protects metadata of real whistleblower messages



Use existing user base to build large anonymity set

Secure Messaging



Embedded and activated in every Guardian app

Cover traffic protects metadata of real whistleblower messages

Use existing user base to build large anonymity set

Strong **plausible deniability** for sources

UNIVERSITY OF CAMBRIDGE

August 2022

sciendo

Proceedings on Privacy Enhancing Technologies ; 2022 (2):47–67

Mansoor Ahmed-Rengers*, Diana A. Vasile*, Daniel Hugenroth*, Alastair R. Beresford, and Ross Anderson

CoverDrop: Blowing the Whistle Through A News App

Abstract: Whistleblowing is hazardous in a world of pervasive surveillance, yet many leading newspapers expect sources to contact them with methods that are either insecure or barely usable. In an attempt to do better, we conducted two workshops with British news organisations and surveyed whistleblowing options and guidelines at major media outlets. We concluded that the soft spot is a system for initial contact and trust establishment between sources and reporters. *CoverDrop* is a two-way, secure system to do this. We support secure messaging within a news app, so that all its other users provide cover traffic, which we channel through a threshold mix instantiated in a Trusted Execution Environment within the news organisation. CoverDrop is designed to resist a powerful global adversary with the ability to issue warrants against infrastructure providers, yet it can easily be integrated into existing infrastructure. We present the results from our workshops, describe CoverDrop's design and demonstrate its security and performance.

Keywords: whistleblowing, anonymous communication, mobile application

DOI 10.2478/popets-2022-0035
Received 2021-08-31; revised 2021-12-15; accepted 2021-12-16.

*Corresponding Author: Mansoor Ahmed-Rengers: OpenOrigins Limited and University of Cambridge, E-mail: Mansoor.Ahmed@cl.cam.ac.uk
*Corresponding Author: Diana A. Vasile: Department of Computer Science and Technology, University of Cambridge, E-mail: Diana.Vasile@cl.cam.ac.uk
*Corresponding Author: Daniel Hugenroth: Department of Computer Science and Technology, University of Cambridge, E-mail: Daniel.Hugenroth@cl.cam.ac.uk
Alastair R. Beresford: Department of Computer Science and Technology, University of Cambridge, E-mail: Alastair.Beresford@cl.cam.ac.uk
Ross Anderson: Department of Computer Science and Technology, University of Cambridge, E-mail: Ross.Anderson@cl.cam.ac.uk

1 Introduction

Since the Snowden leaks [15], newspapers and their potential sources have become aware of the mass-surveillance infrastructure available to nation states. This has profound implications for those who wish to expose wrongdoing within government, and in organisations that can call on its assistance.

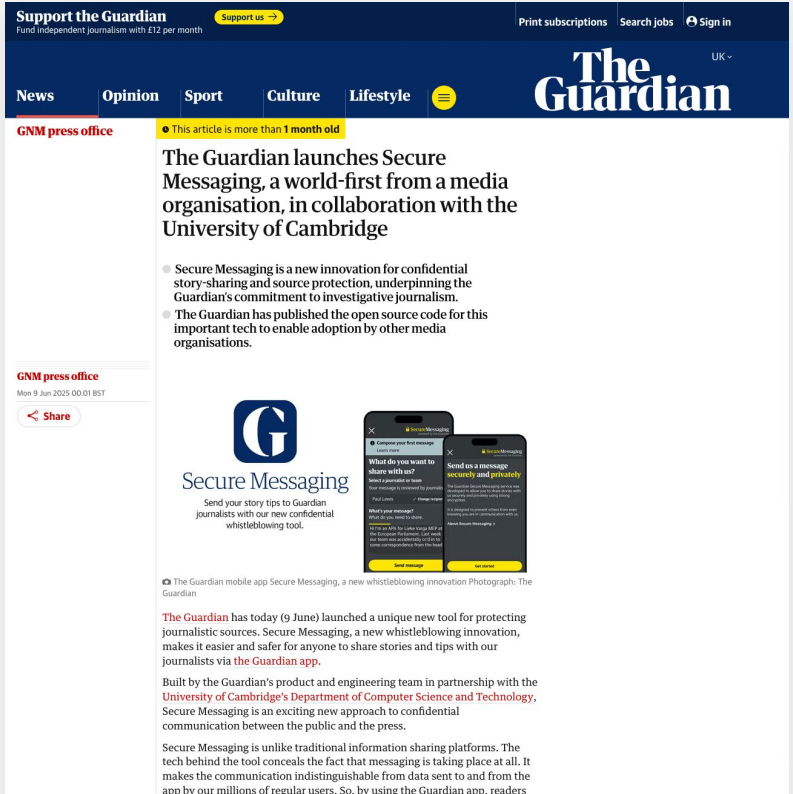
Whistleblowers may face severe penalties if caught: in the recent past, they have been physically intimidated [28], imprisoned [46, 51], and even assassinated [43]. Even in less extreme cases, they face dismissal [35], litigation, and professional boycotts [41]. Yet, whistleblowing is often the last line of defence against unethical or illegal behaviour by the powerful. In the context of government agencies, it may be the principal means of exposing crimes that may have been covered up under the guise of national security. It is also widely recognised as a crucial component in accountability, and many countries have explicit laws for protecting whistleblowers. Unfortunately, these laws have proven to be insufficient in many recent cases. Since the Snowden revelations, we have seen the emergence of tools such as SecureDrop, and many major news organisations have web pages to advise whistleblowers on how to contact them securely with sensitive information. A preliminary examination convinced us that the tools are often hard to use securely and the advice inadequate. How could we do better?

In order to understand the whistleblowing process in the real world, we conducted two workshops with journalists and IT staff at news organisations. These workshops provided valuable insights into the practical difficulties of supporting whistleblowers and how journalists work with them. The main lesson we drew from these workshops was that there is no secure way for whistleblowers to initiate contact with reporters. Consequently, initial contact is undertaken via insecure means and only later escalated to more secure channels (e.g., SecureDrop), by which point it may already be too late.

In this paper, we present *CoverDrop*, a system which helps potential whistleblowers securely initiate contact and whose design emerged from these discus-

CC BY-NC-ND

June 2025



Support the Guardian
Fund independent journalism with £12 per month
Support us
Print subscriptions | Search jobs | Sign in

The Guardian
UK

News | Opinion | Sport | Culture | Lifestyle

GNM press office

This article is more than 1 month old

The Guardian launches Secure Messaging, a world-first from a media organisation, in collaboration with the University of Cambridge

- Secure Messaging is a new innovation for confidential story-sharing and source protection, underpinning the Guardian's commitment to investigative journalism.
- The Guardian has published the open source code for this important tech to enable adoption by other media organisations.

GNM press office
Mon 9 Jun 2025 00.01 BST

Share

Secure Messaging
Send your story tips to Guardian journalists with our new confidential whistleblowing tool.

The Guardian mobile app Secure Messaging, a new whistleblowing innovation Photograph: The Guardian

The Guardian has today (9 June) launched a unique new tool for protecting journalistic sources. Secure Messaging, a new whistleblowing innovation, makes it easier and safer for anyone to share stories and tips with our journalists via the Guardian app.

Built by the Guardian's product and engineering team in partnership with the University of Cambridge's Department of Computer Science and Technology, Secure Messaging is an exciting new approach to confidential communication between the public and the press.

Secure Messaging is unlike traditional information sharing platforms. The tech behind the tool conceals the fact that messaging is taking place at all. It makes the communication indistinguishable from data sent to and from the app by our millions of regular users. So, by using the Guardian app, readers

“The quality of incoming messages is incomparable to what came before.”

—Deputy Investigations Editor

Threat model and assumptions.

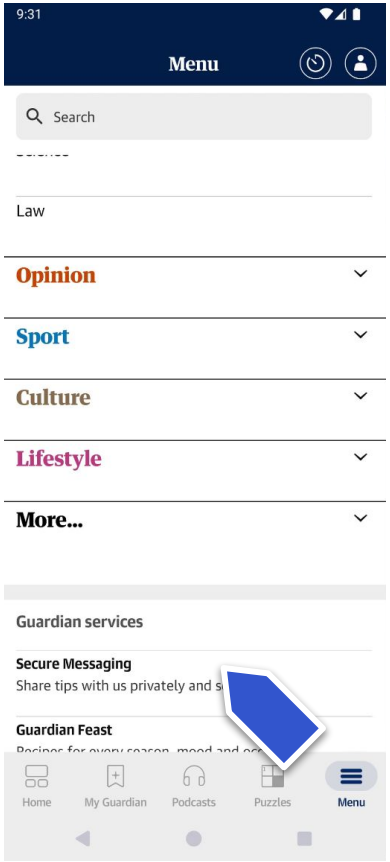
😈 **Compromise cloud providers**

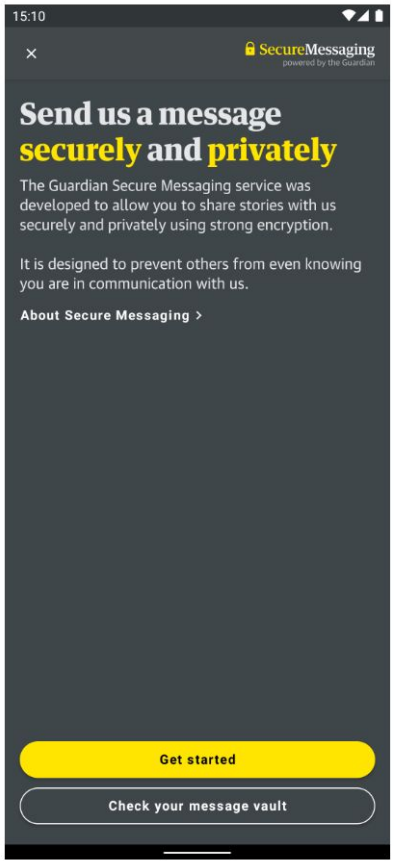
😈 Observe, record, or modify Internet traffic at scale

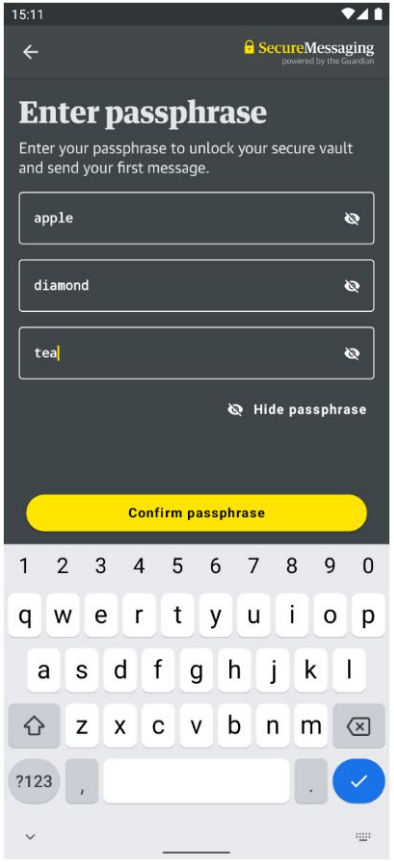
😈 Capture sources' smartphones

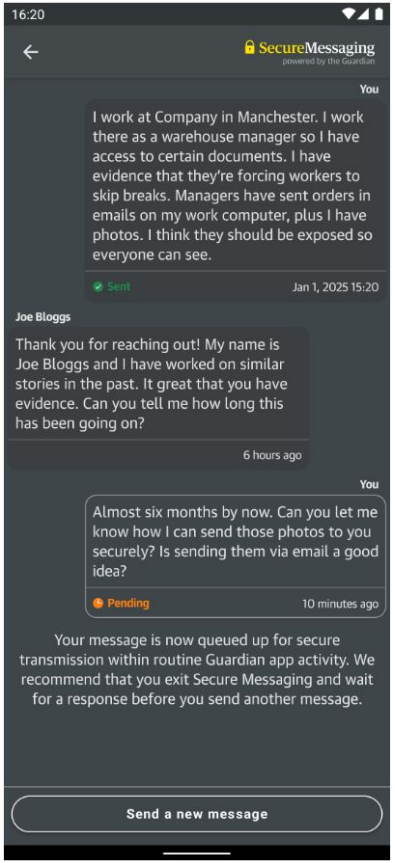
✅ The news organisation runs nodes in a **physically-secure location**.

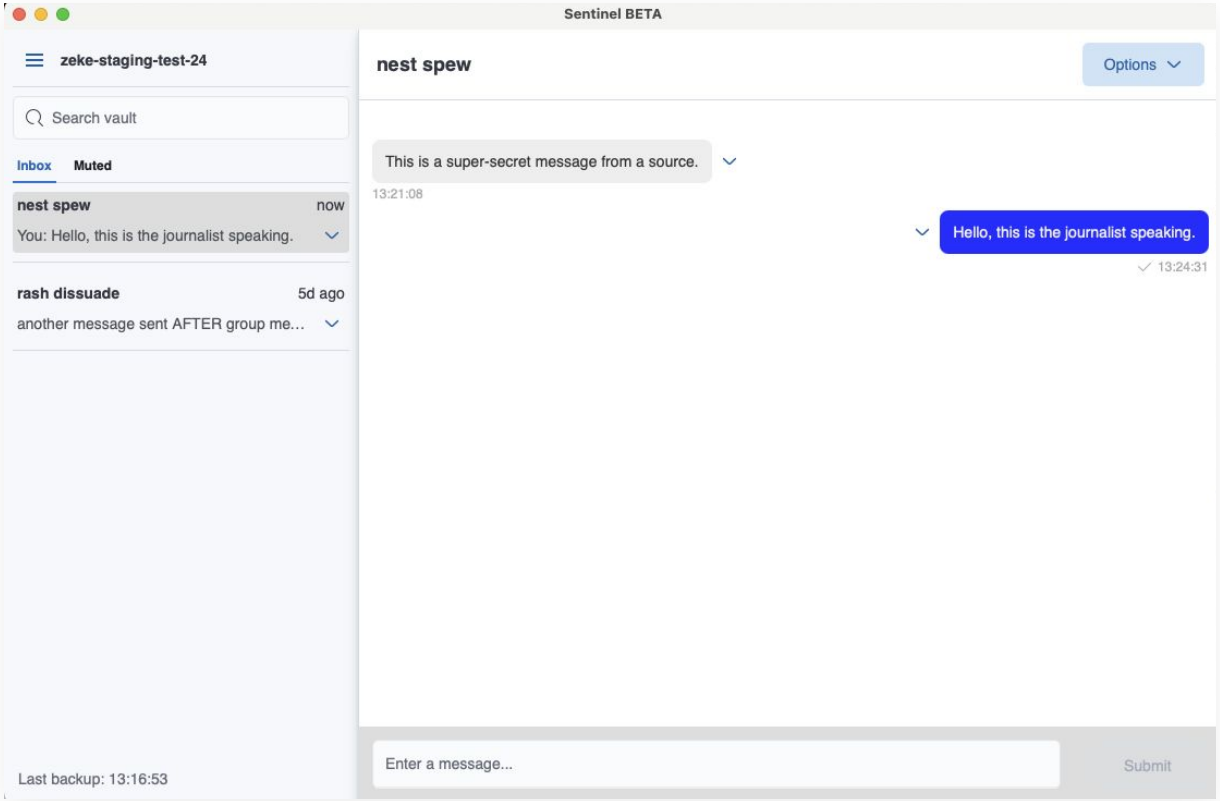
✅ Source and journalist devices are not compromised with malware


9:31
Menu
Search
Law
Opinion
Sport
Culture
Lifestyle
More...
Guardian services
Secure Messaging
Guardian Feast
Home
My Guardian
Podcasts
Puzzles
Menu


15:10
SecureMessaging
powered by the Guardian
Send us a message securely and privately
The Guardian Secure Messaging service was developed to allow you to share stories with us securely and privately using strong encryption.
It is designed to prevent others from even knowing you are in communication with us.
About Secure Messaging ›
Get started
Check your message vault


15:11
SecureMessaging
powered by the Guardian
Enter passphrase
Enter your passphrase to unlock your secure vault and send your first message.
apple
diamond
tea
Hide passphrase
Confirm passphrase
1 2 3 4 5 6 7 8 9 0
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
?123


16:20
SecureMessaging
powered by the Guardian
You
I work at Company in Manchester. I work there as a warehouse manager so I have access to certain documents. I have evidence that they're forcing workers to skip breaks. Managers have sent orders in emails on my work computer, plus I have photos. I think they should be exposed so everyone can see.
Sent
Jan 1, 2025 15:20
Joe Bloggs
Thank you for reaching out! My name is Joe Bloggs and I have worked on similar stories in the past. It great that you have evidence. Can you tell me how long this has been going on?
6 hours ago
You
Almost six months by now. Can you let me know how I can send those photos to you securely? Is sending them via email a good idea?
Pending
10 minutes ago
Your message is now queued up for secure transmission within routine Guardian app activity. We recommend that you exit Secure Messaging and wait for a response before you send another message.
Send a new message



TAURI

SQLite

SQL CIPHER

Post-launch timeline

Secure Messaging launched

June 2025

Post-launch timeline

Secure Messaging launched

June 2025

E2EE Journalist vault backups

November 2025

Post-launch timeline

Secure Messaging launched

June 2025

E2EE Journalist vault backups

November 2025

Group messaging

2026

Post-launch timeline

Secure Messaging launched

June 2025

E2EE Journalist vault backups

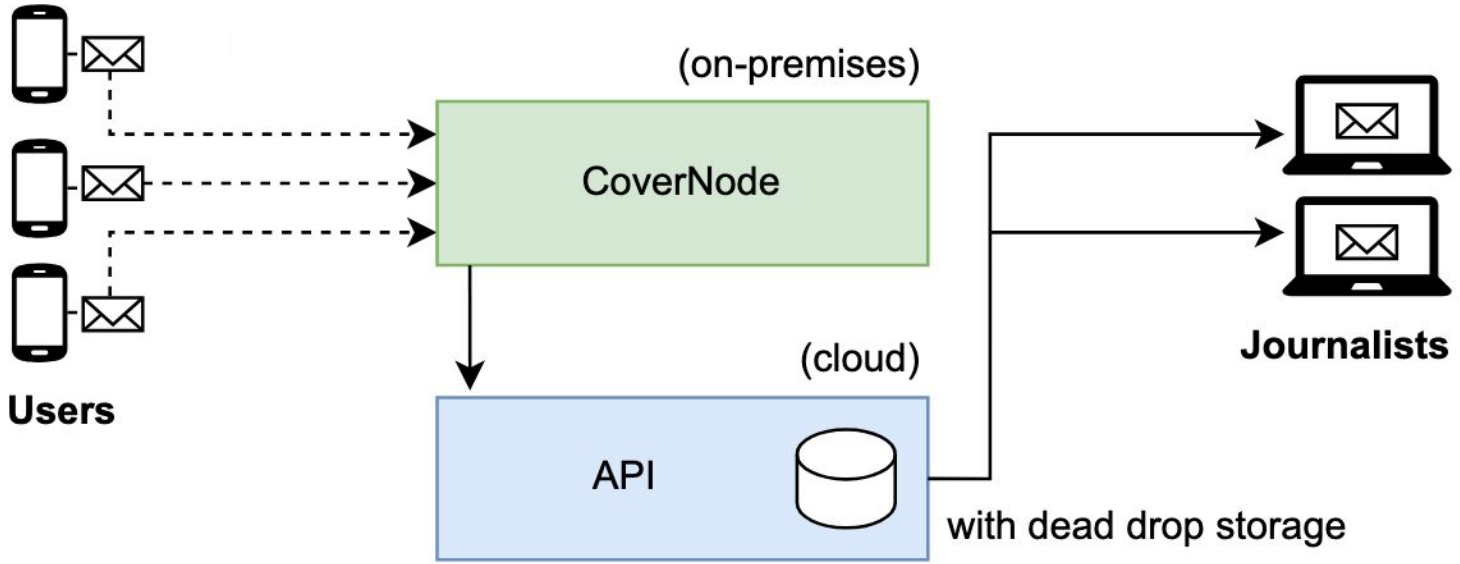
November 2025

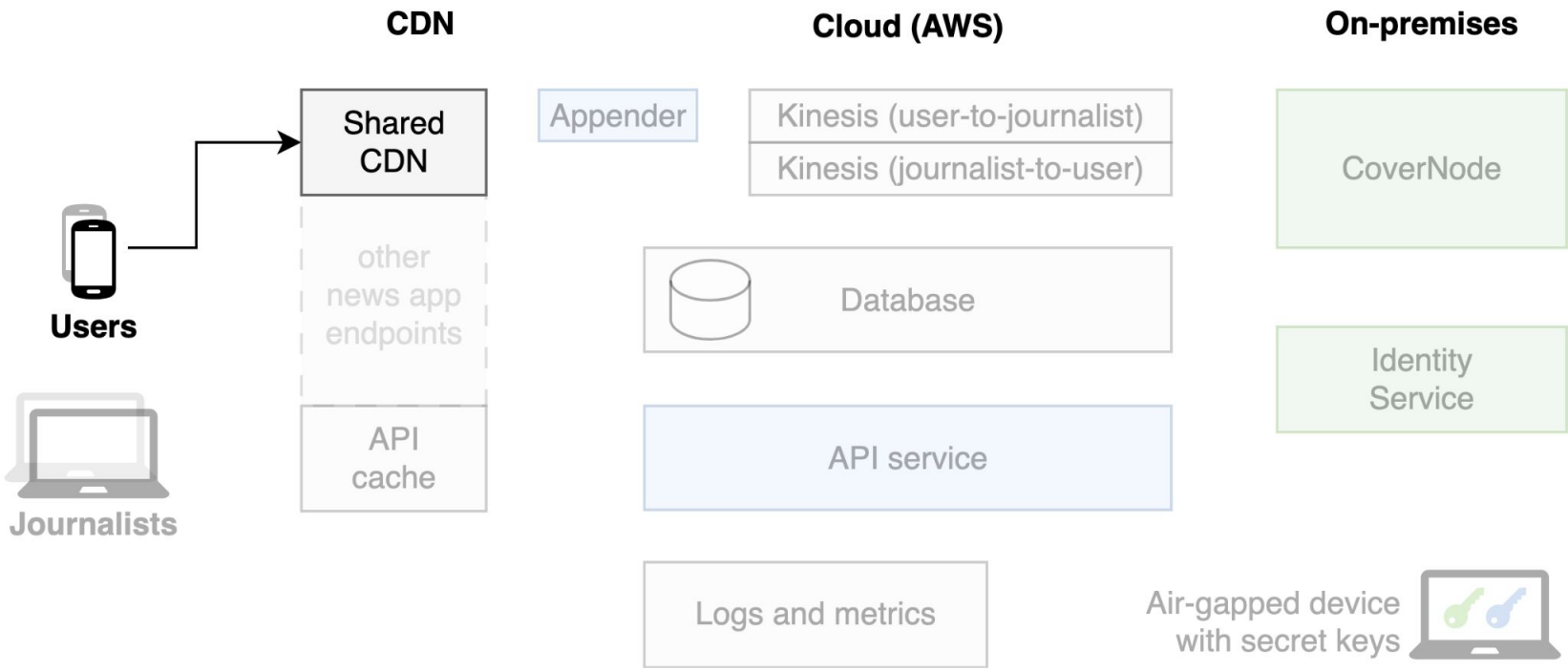
Group messaging

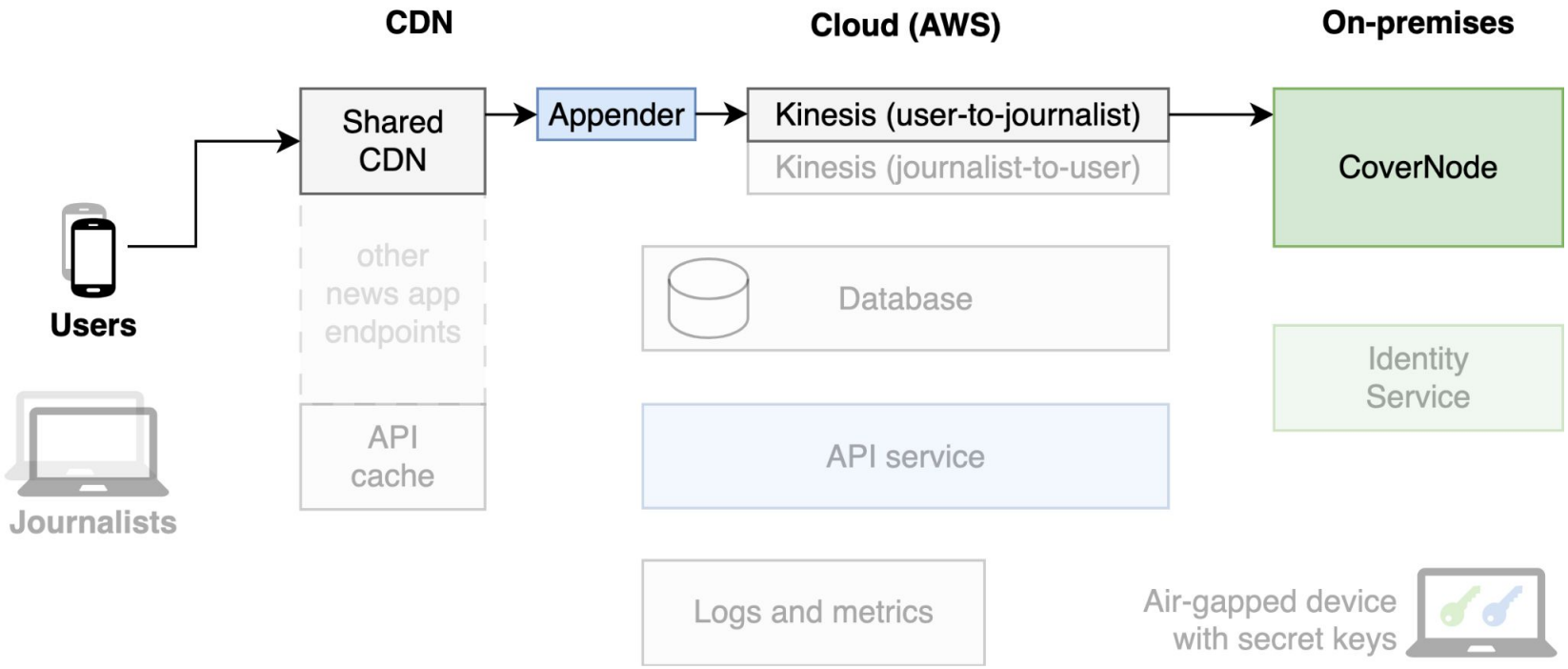
2026

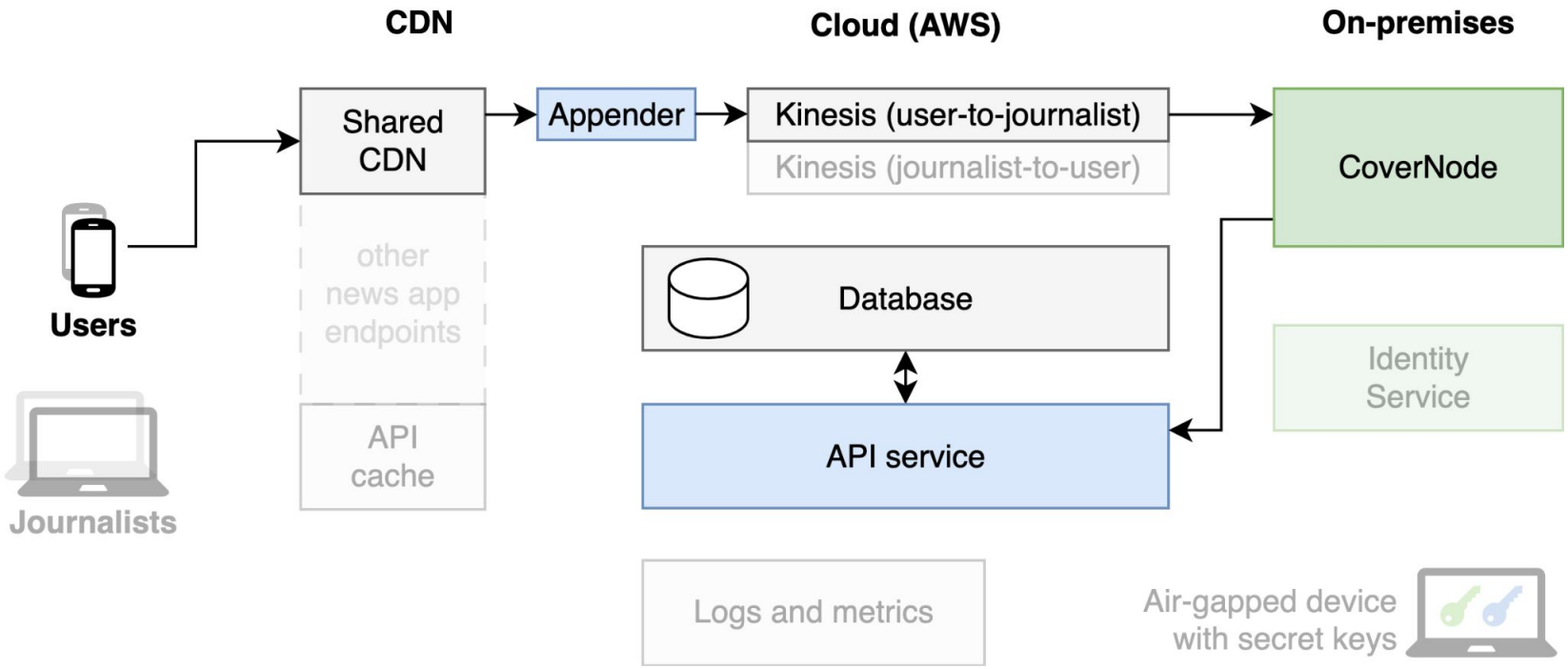
Post quantum CoverDrop

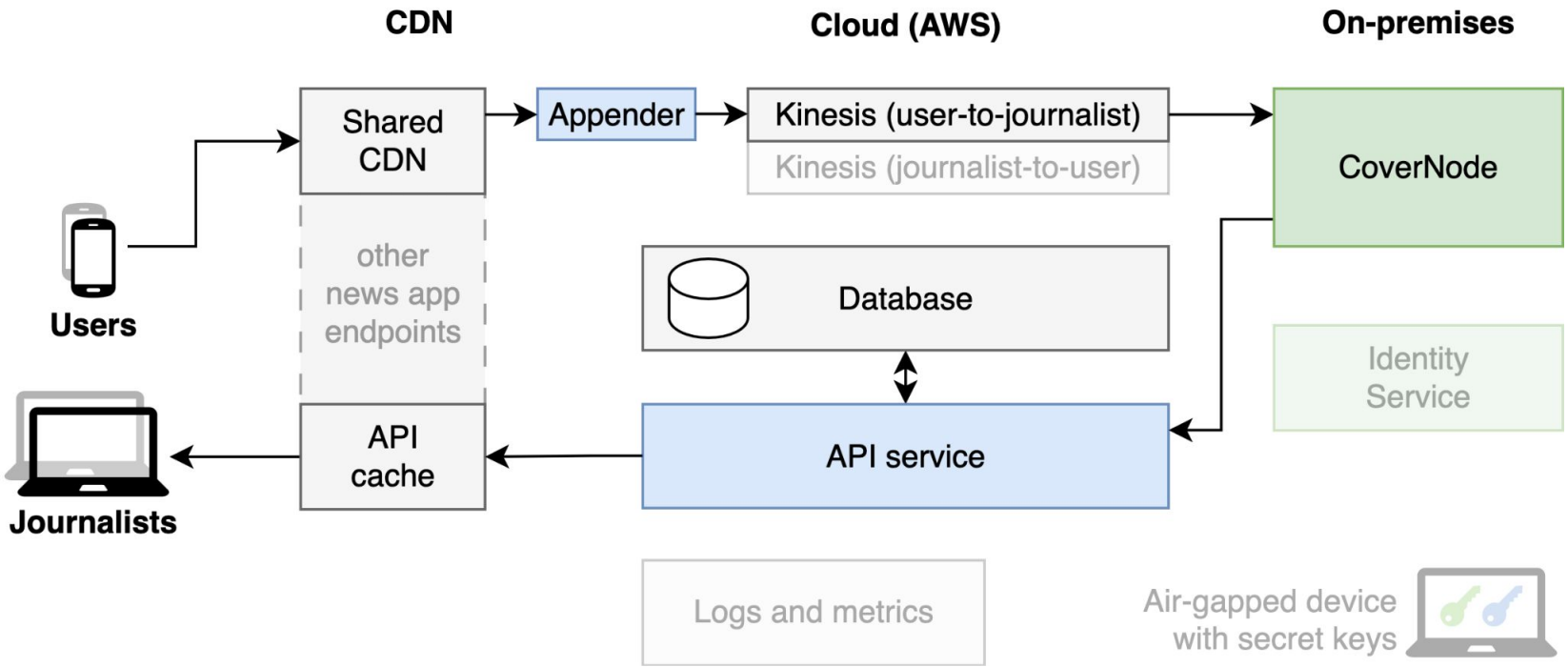
2027

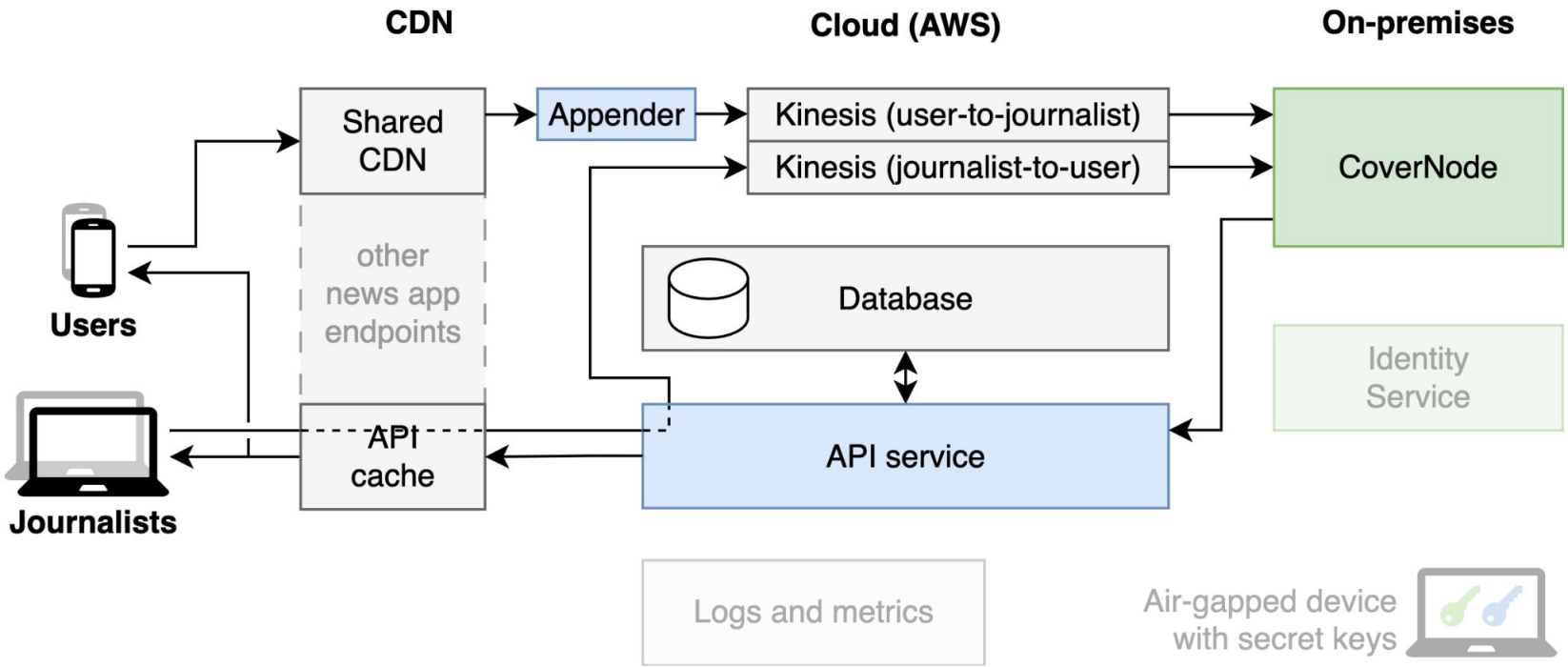

(on-premises)
CoverNode
(cloud)
API
with dead drop storage
Users
Journalists

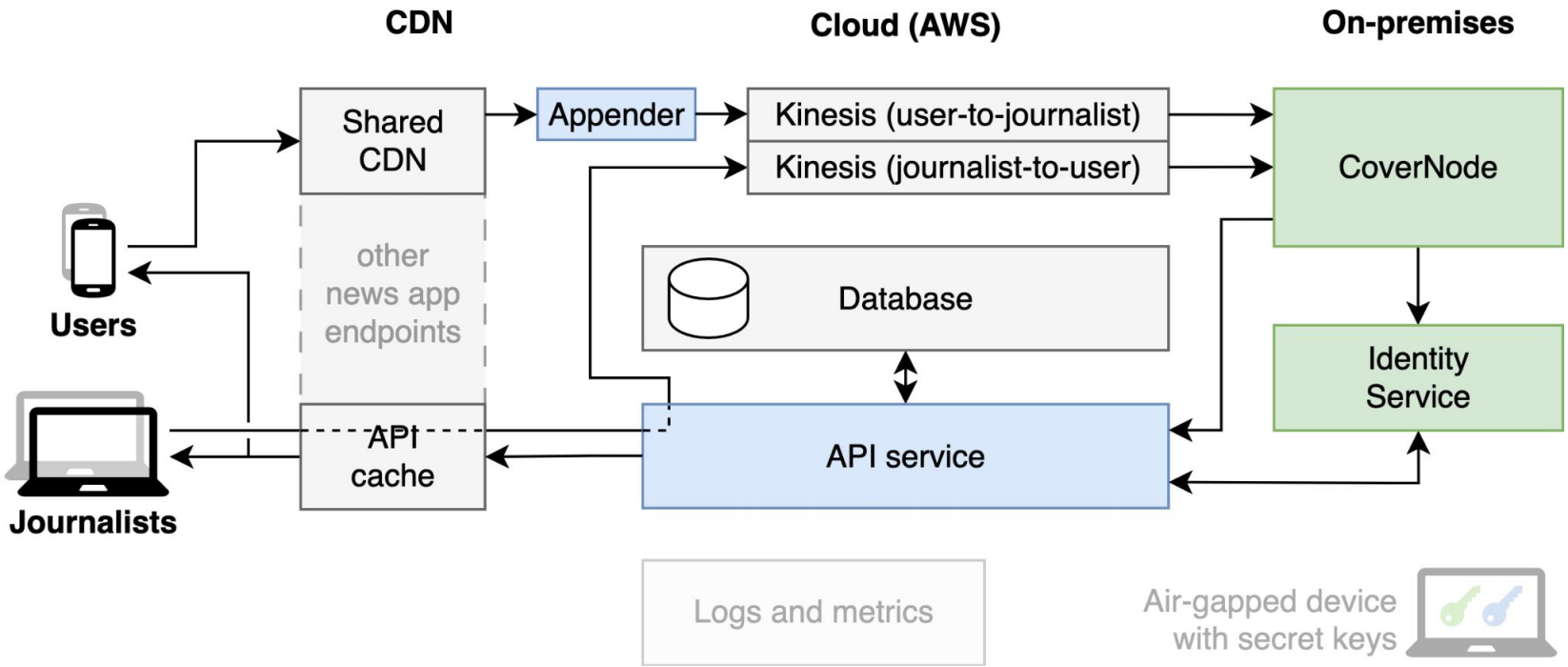

CDN
Cloud (AWS)
On-premises
Shared CDN
other news app endpoints
API cache
Users
Journalists
Appender
Kinesis (user-to-journalist)
Kinesis (journalist-to-user)
Database
API service
Logs and metrics
CoverNode
Identity Service
Air-gapped device with secret keys

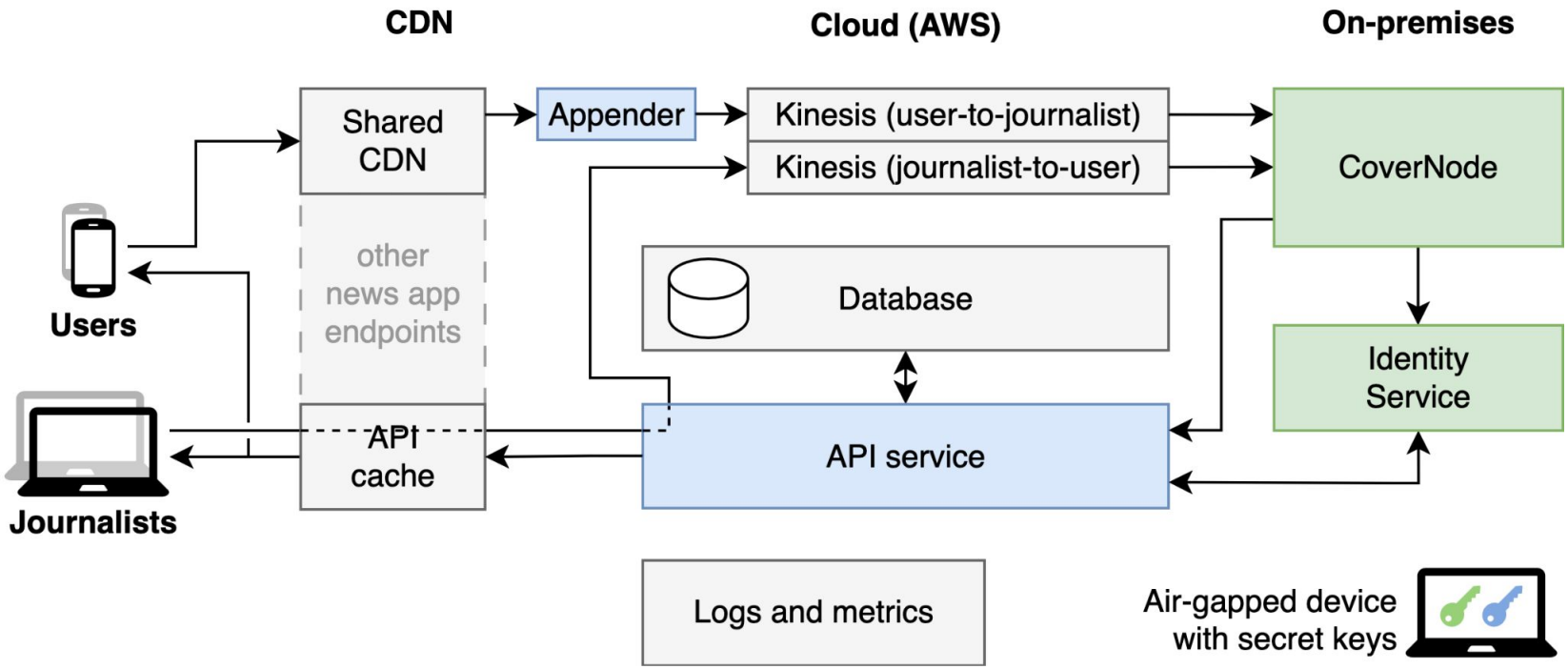

CDN
Cloud (AWS)
On-premises
Shared CDN
Appender
Kinesis (user-to-journalist)
Kinesis (journalist-to-user)
CoverNode
Users
other news app endpoints
Database
Identity Service
Journalists
API cache
API service
Logs and metrics
Air-gapped device with secret keys


CDN
Cloud (AWS)
On-premises
Shared CDN
Appender
Kinesis (user-to-journalist)
Kinesis (journalist-to-user)
CoverNode
Users
other news app endpoints
Database
Identity Service
API cache
API service
Journalists
Logs and metrics
Air-gapped device with secret keys


CDN
Cloud (AWS)
On-premises
Shared CDN
Appender
Kinesis (user-to-journalist)
Kinesis (journalist-to-user)
CoverNode
Users
other news app endpoints
Database
Identity Service
API cache
API service
Journalists
Logs and metrics
Air-gapped device with secret keys


CDN
Cloud (AWS)
On-premises
Shared CDN
Appender
Kinesis (user-to-journalist)
Kinesis (journalist-to-user)
CoverNode
other news app endpoints
Database
Identity Service
Users
API cache
API service
Journalists
Logs and metrics
Air-gapped device with secret keys


CDN
Cloud (AWS)
On-premises
Shared CDN
Appender
Kinesis (user-to-journalist)
Kinesis (journalist-to-user)
CoverNode
other news app endpoints
Database
Identity Service
Users
API cache
API service
Journalists
Logs and metrics
Air-gapped device with secret keys

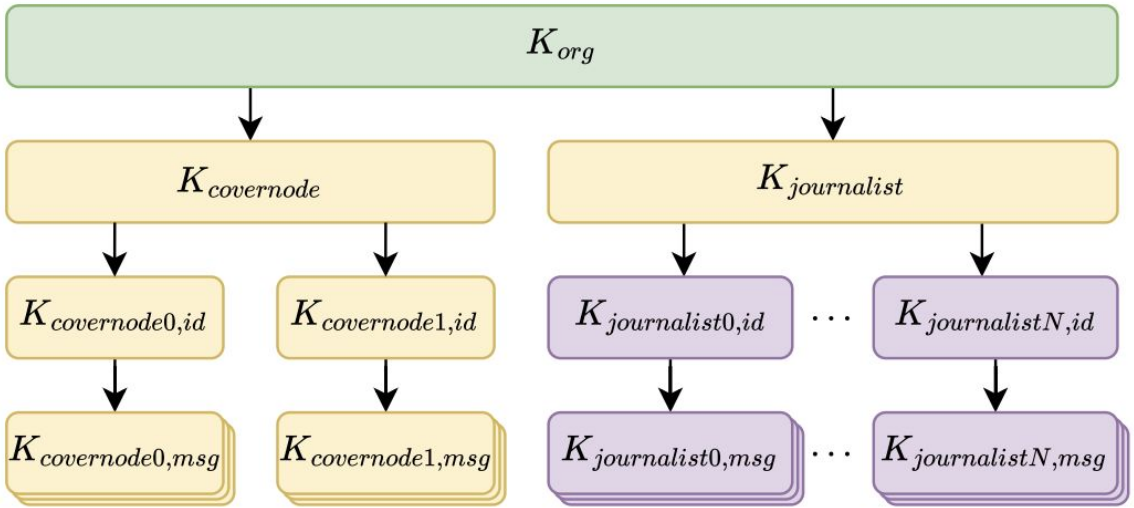

CDN
Cloud (AWS)
On-premises
Shared CDN
Appender
Kinesis (user-to-journalist)
Kinesis (journalist-to-user)
CoverNode
other news app endpoints
Database
Identity Service
Users
API cache
API service
Journalists
Logs and metrics
Air-gapped device with secret keys

Organisation

Provisioning

Identity

Messaging

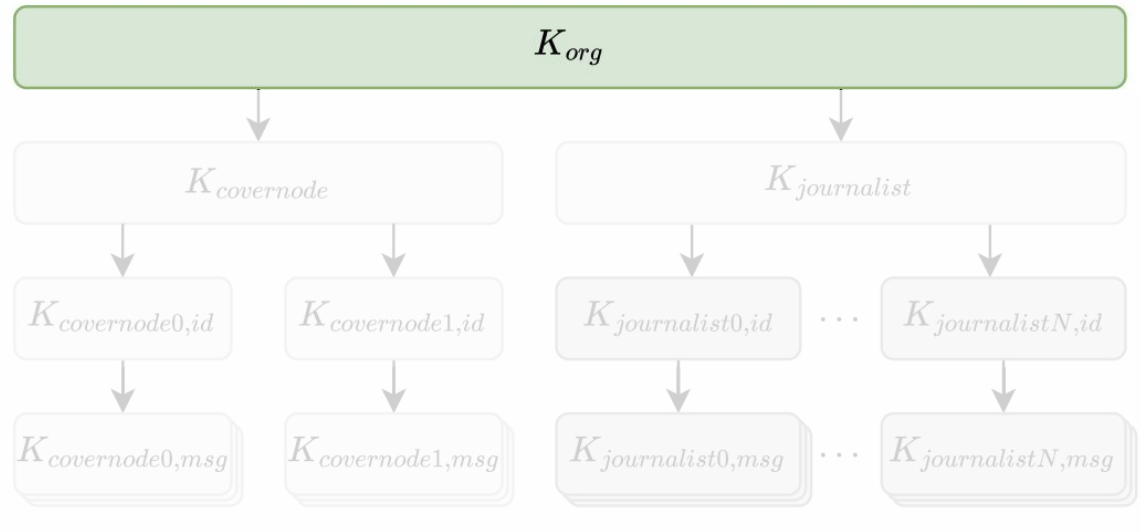


Organisation

Provisioning

Identity

Messaging

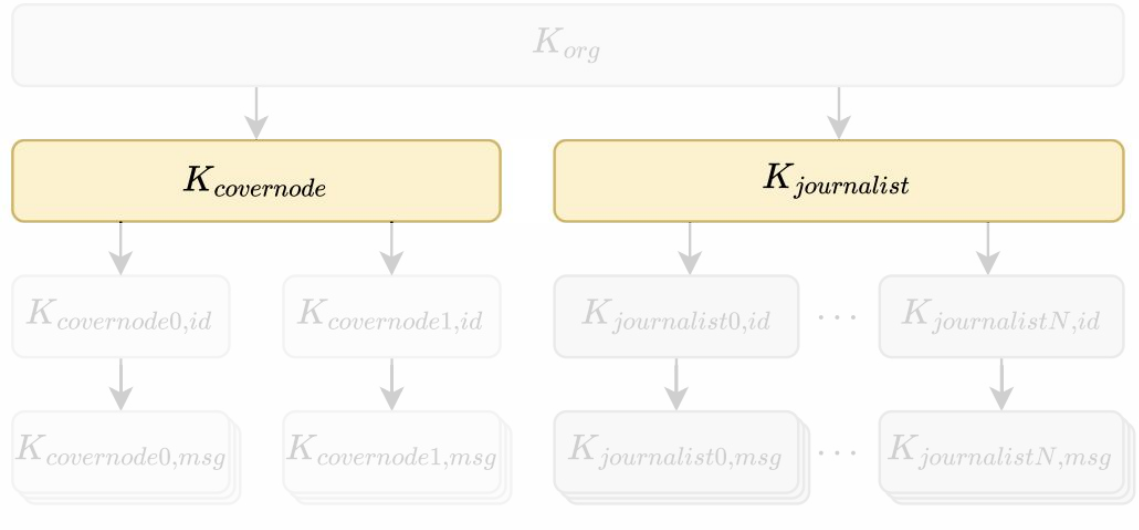


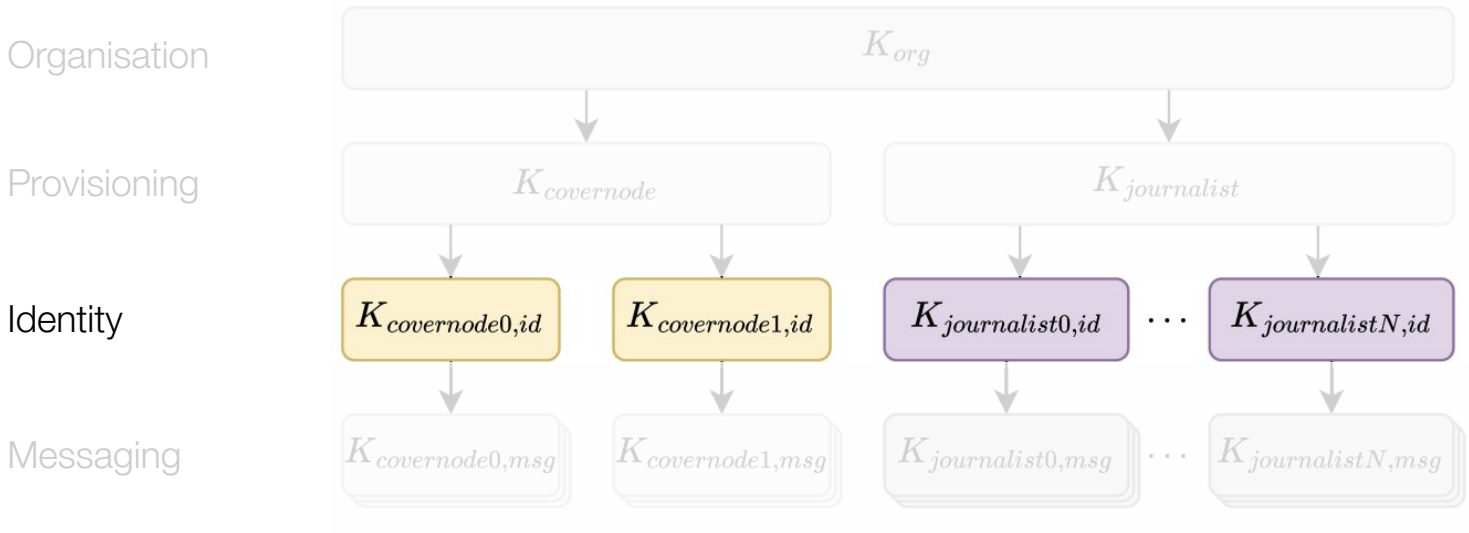
Organisation

Provisioning

Identity

Messaging



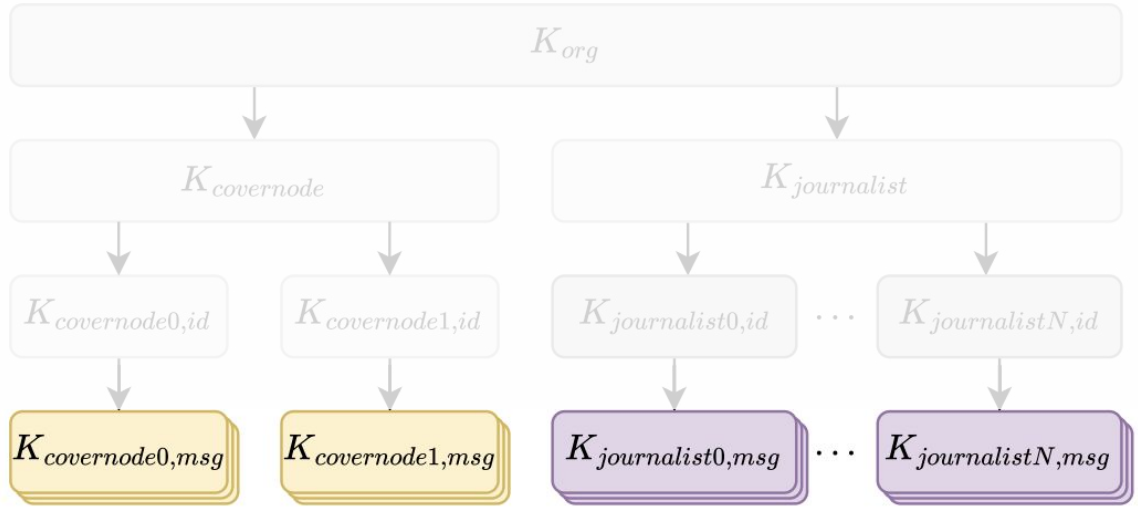

Organisation
Provisioning
Identity
Messaging
K_{org}
$K_{covernode}$
$K_{journalist}$
$K_{covernode0,id}$
$K_{covernode1,id}$
$K_{journalist0,id}$
$\cdots$
$K_{journalistN,id}$
$K_{covernode0,msg}$
$K_{covernode1,msg}$
$K_{journalist0,msg}$
$\cdots$
$K_{journalistN,msg}$

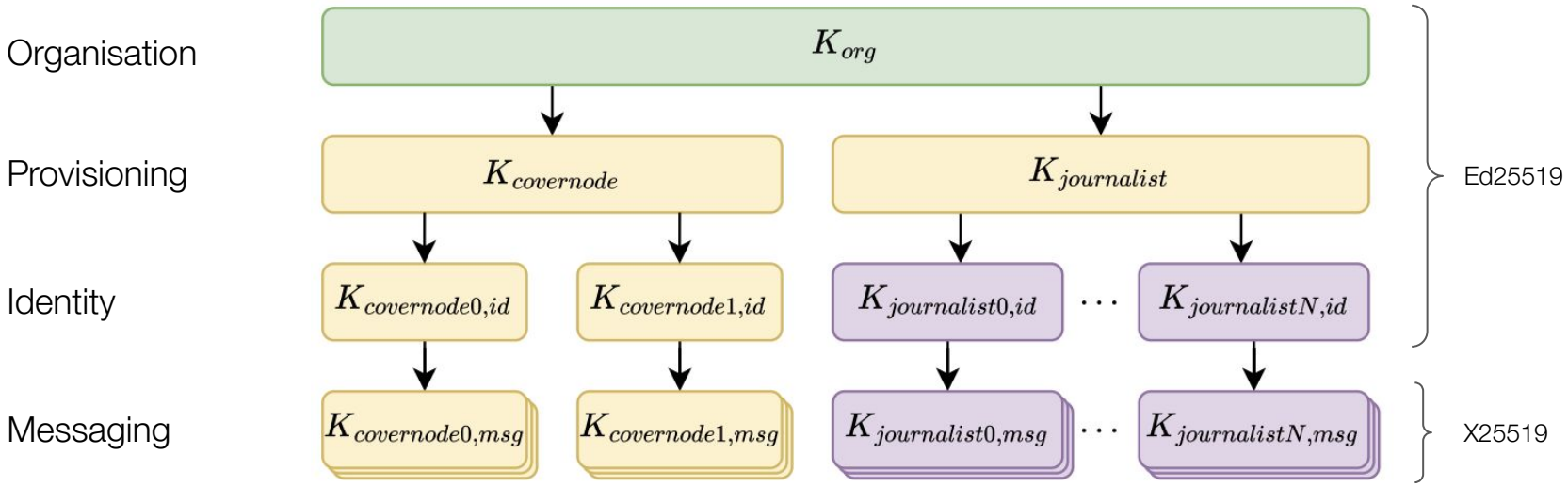
Organisation

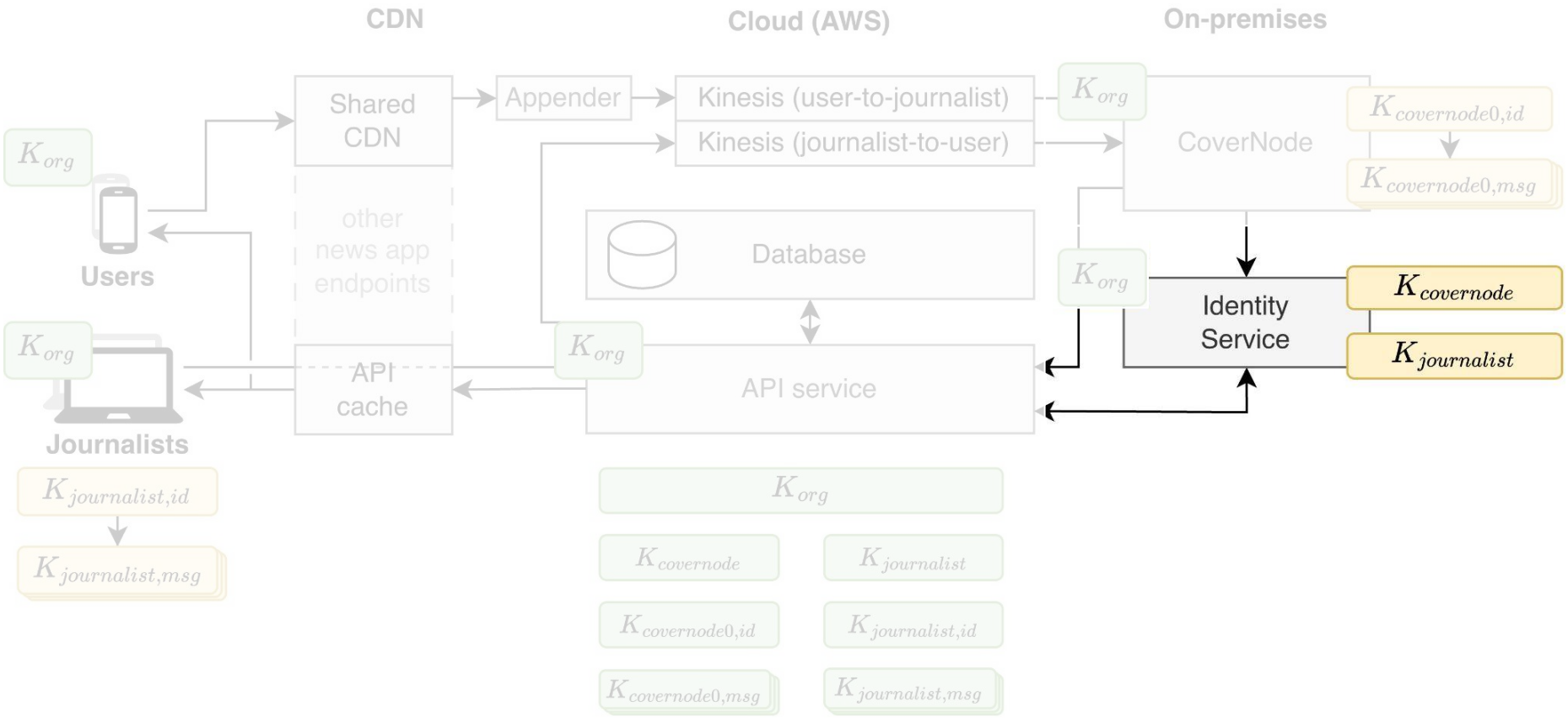
Provisioning

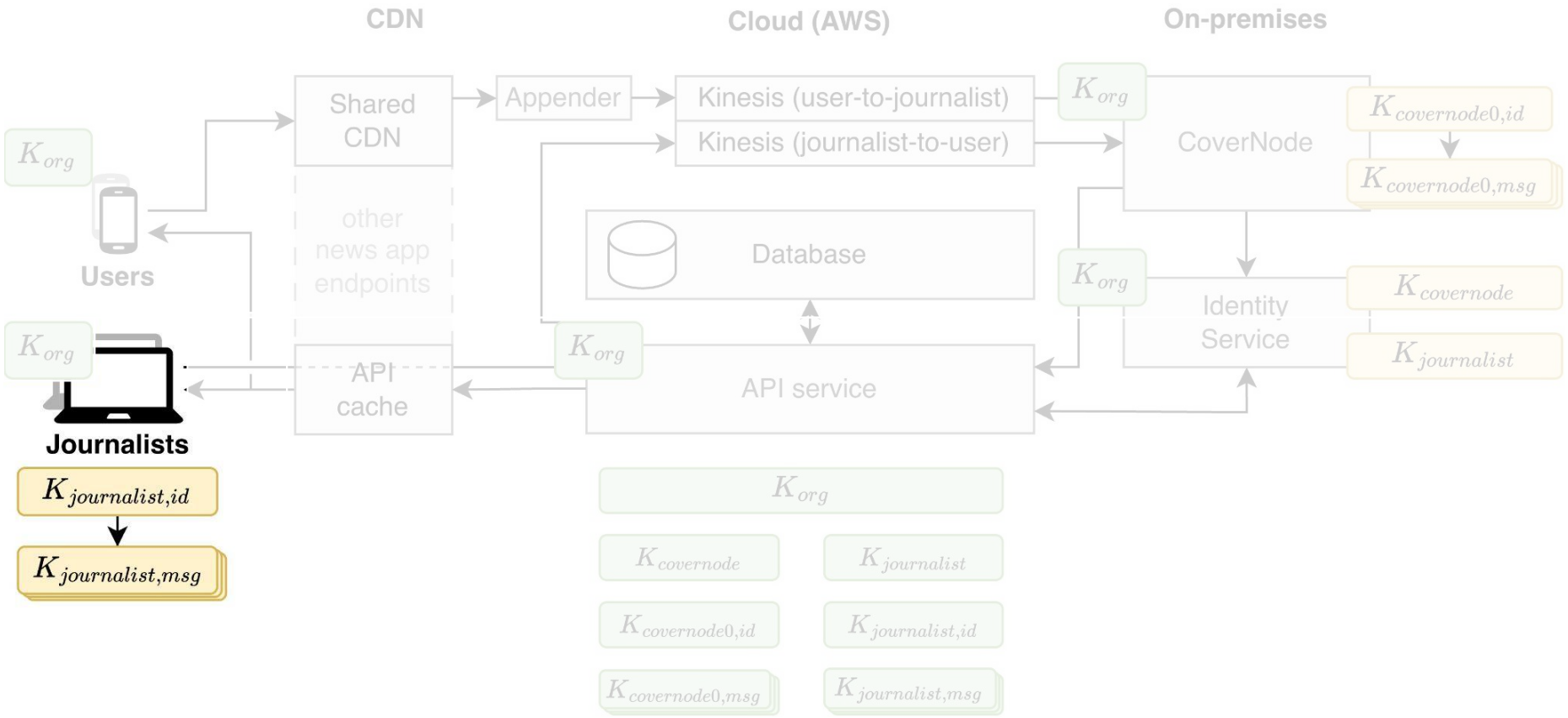
Identity

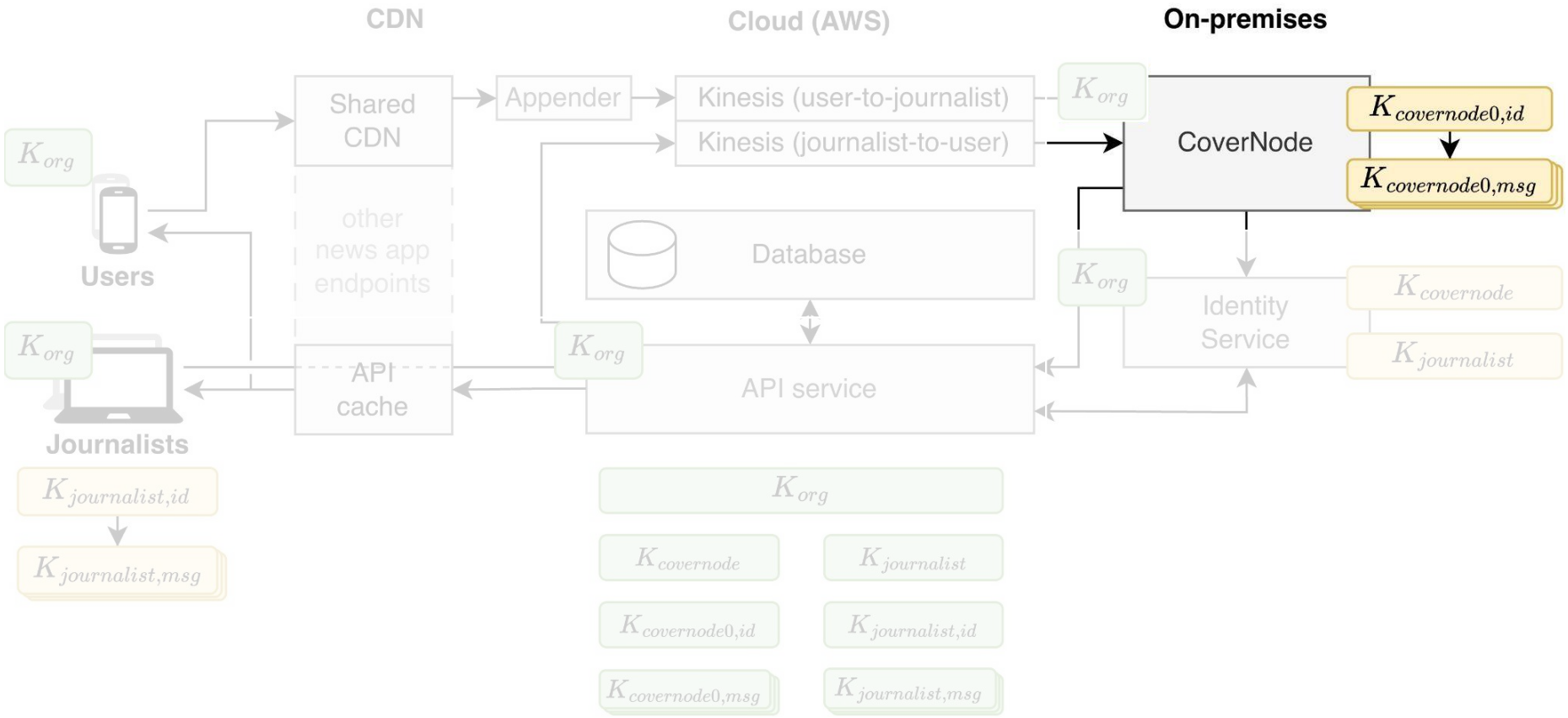
Messaging

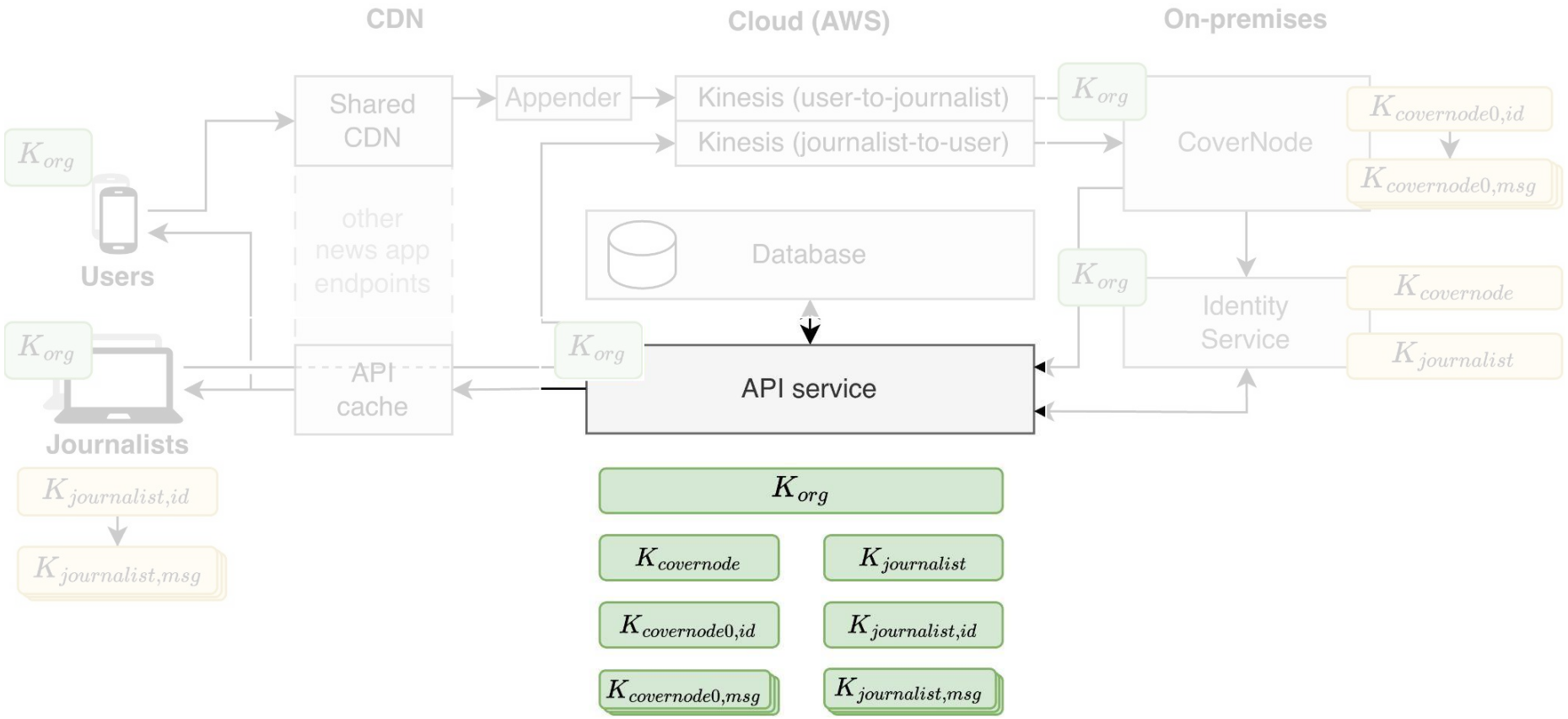


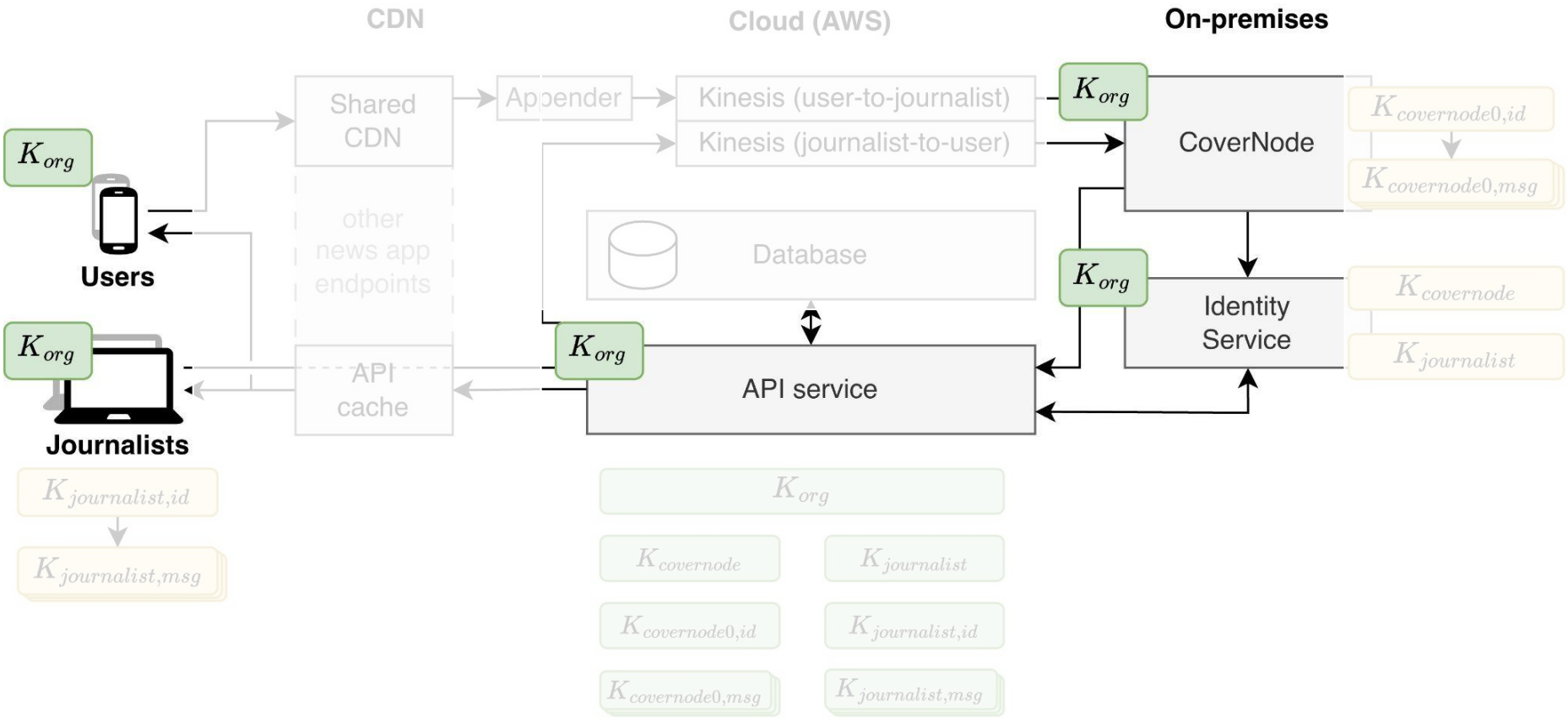

Organisation
Provisioning
Identity
Messaging
K_{org}
$K_{covernode}$
$K_{journalist}$
$K_{covernode0,id}$
$K_{covernode1,id}$
$K_{journalist0,id}$
$K_{journalistN,id}$
$K_{covernode0,msg}$
$K_{covernode1,msg}$
$K_{journalist0,msg}$
$K_{journalistN,msg}$
Ed25519
X25519


CDN
Cloud (AWS)
On-premises
Shared CDN
Appender
Kinesis (user-to-journalist)
Kinesis (journalist-to-user)
CoverNode
other news app endpoints
Database
Identity Service
API cache
API service
Users
Journalists
K_{org}
$K_{covernode0,id}$
$K_{covernode0,msg}$
$K_{covernode}$
$K_{journalist}$
$K_{journalist,id}$
$K_{journalist,msg}$


CDN
Cloud (AWS)
On-premises
Shared CDN
Appender
Kinesis (user-to-journalist)
Kinesis (journalist-to-user)
CoverNode
other news app endpoints
Database
Identity Service
API cache
API service
Users
Journalists
K_{org}
$K_{covernode0,id}$
$K_{covernode0,msg}$
$K_{covernode}$
$K_{journalist}$
$K_{journalist,id}$
$K_{journalist,msg}$

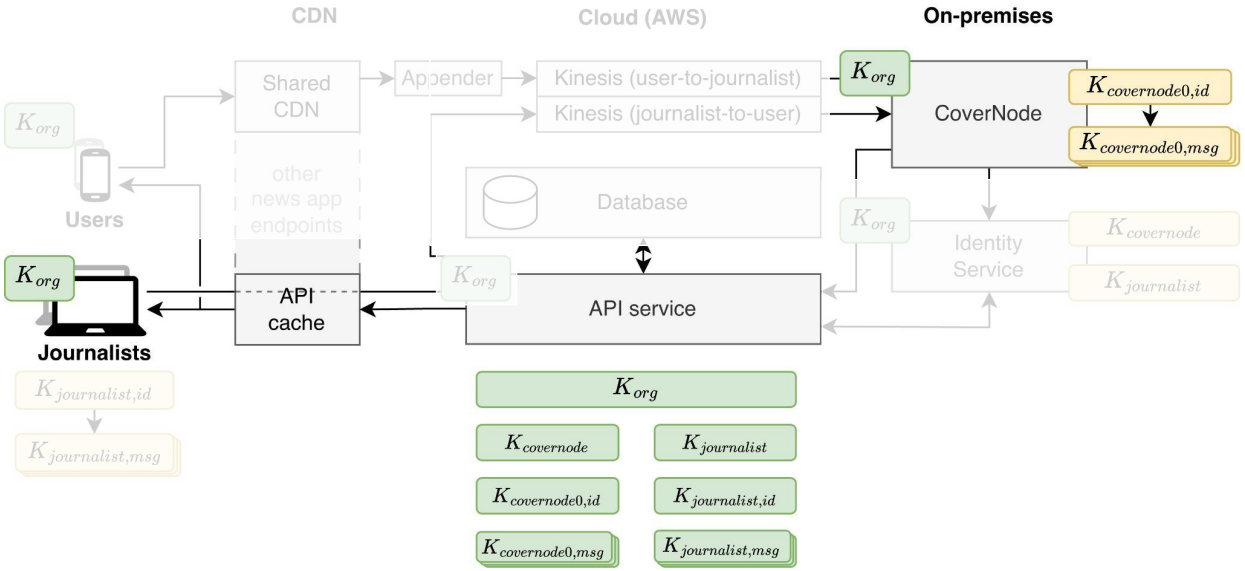

CDN
Cloud (AWS)
On-premises
Shared CDN
Appender
Kinesis (user-to-journalist)
Kinesis (journalist-to-user)
CoverNode
other news app endpoints
Database
Identity Service
Users
API cache
API service
Journalists


CDN
Cloud (AWS)
On-premises
Shared CDN
Appender
Kinesis (user-to-journalist)
Kinesis (journalist-to-user)
CoverNode
other news app endpoints
Database
Identity Service
Users
API cache
API service
Journalists
K_{org}
$K_{covernode0,id}$
$K_{covernode0,msg}$
$K_{covernode}$
$K_{journalist}$
$K_{journalist,id}$
$K_{journalist,msg}$


CDN
Cloud (AWS)
On-premises
Shared CDN
Appender
Kinesis (user-to-journalist)
Kinesis (journalist-to-user)
CoverNode
other news app endpoints
Database
Identity Service
API cache
API service
Users
Journalists
K_{org}
$K_{covernode0,id}$
$K_{covernode0,msg}$
$K_{covernode}$
$K_{journalist}$
$K_{journalist,id}$
$K_{journalist,msg}$

Example of key hierarchy in use: Sentinel verifying a dead drop

- Download public key hierarchy from the API
- Verify hierarchy against trust anchor
- Find all verified CoverNode id public keys
- Attempt to verify the dead drop with each



A printed out-of-band root of trust for the key hierarchy.

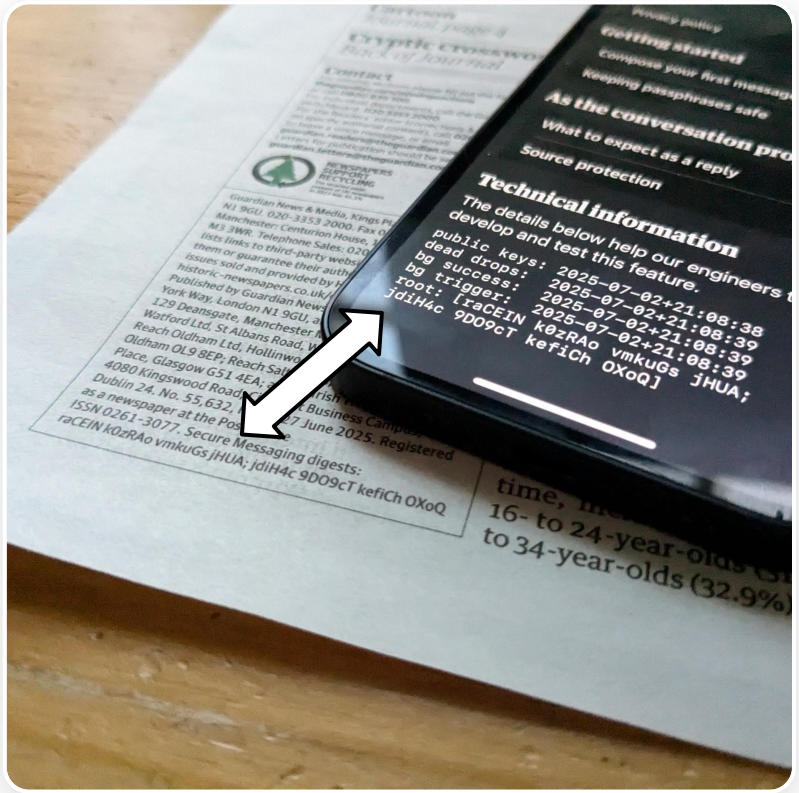


Photo by Grigorii Shcheglov on Unsplash

Questions?

Group messaging in Sentinel

Drawbacks of 1:1 messaging

Editors want to share management of profiles

Sources don’t always choose the journalist best placed to handle their tip

Journalists take sabbaticals, go on holiday, get sick, etc.

Requirements for group messaging

- 🤝 **Delegate source conversations**
- 💼 **Share ownership of journalist profiles**
- 🚚 **No more transferring vaults**
- 🔀 **Other organisations can opt out**

Goal: shared management of journalist profiles, and source conversations

MLS

Messaging Layer Security (RFC 9420)

- Encrypted messaging protocol providing continuous group authenticated key exchange
- Scales to 10s of thousands of users per group
- Growing adoption

- Message confidentiality
- Integrity and authentication
- Asynchronicity
- Forward secrecy (FS)
- Post-compromise security (PCS)

webex by CISCO wire XMTP RCS matrix

MLS Protocol overview

GROUP

Group are collection of **clients.**

GROUP SECRET

Group secret evolves through **epochs** as membership changes.

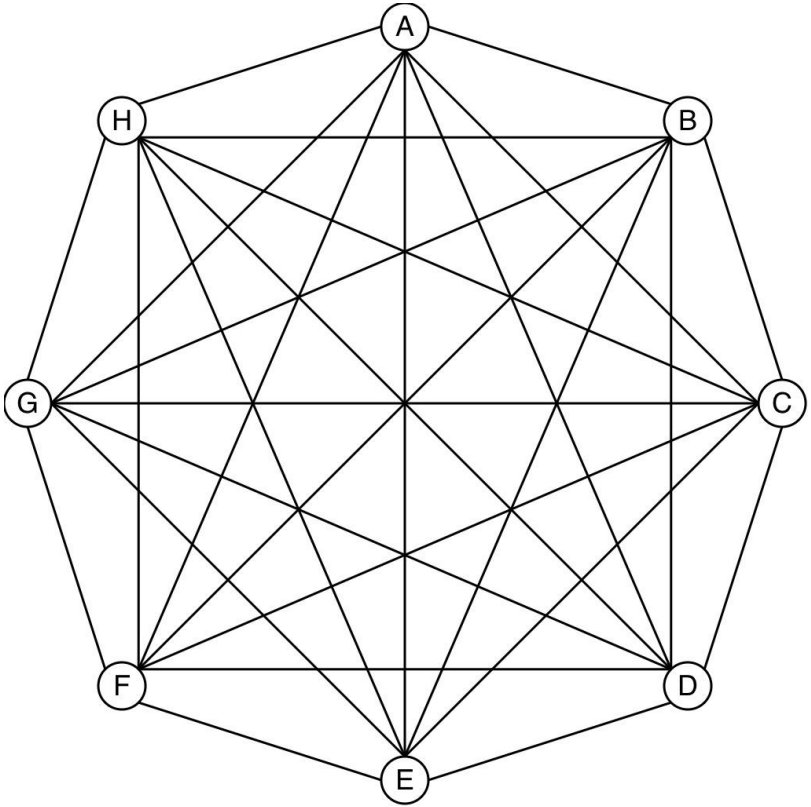
CLIENTS

Clients represented by a **credential** and a **signing key.**

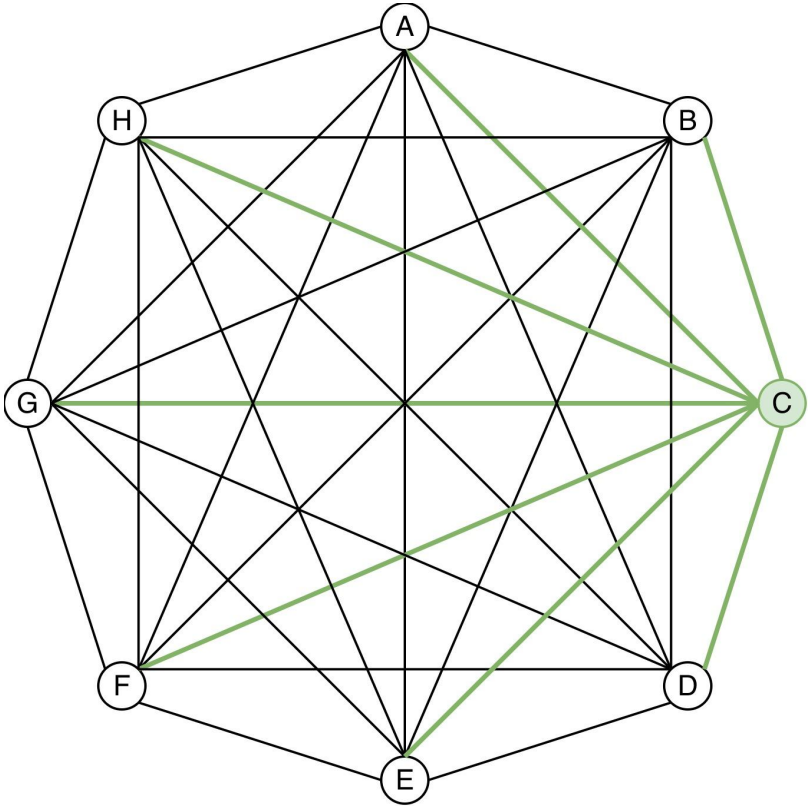
RATCHET TREE

Ratchet tree used to efficiently encrypt for a subset of clients.

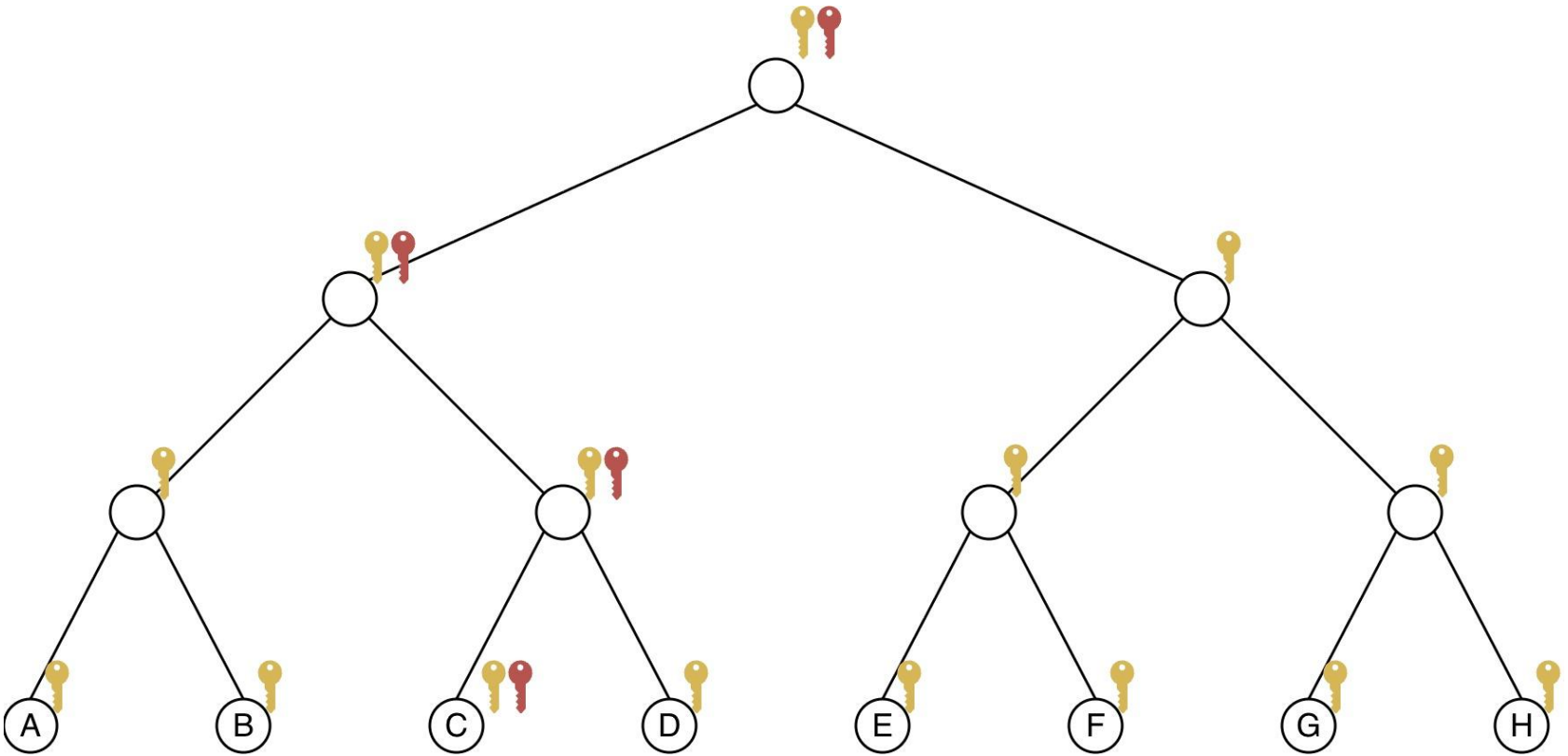
Pairwise encryption



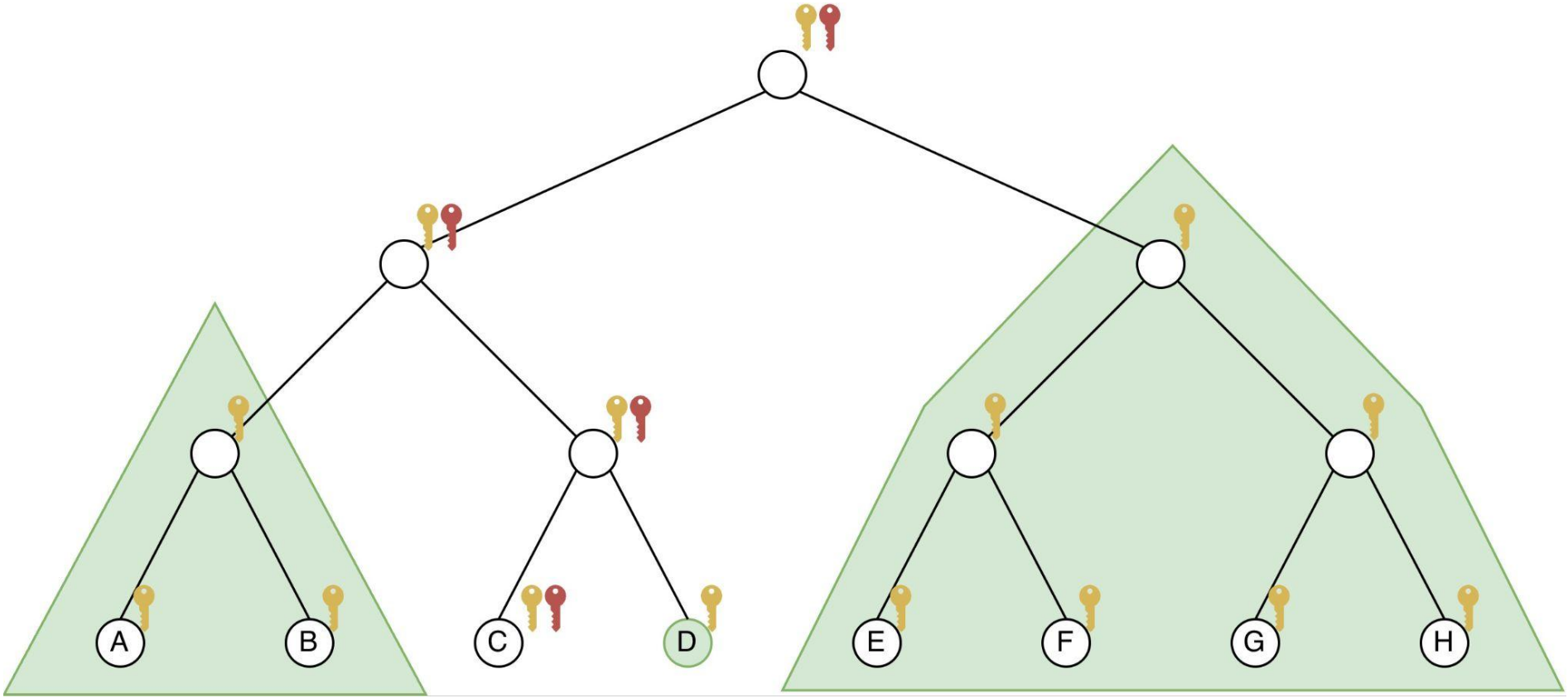
Pairwise encryption



Ratchet tree

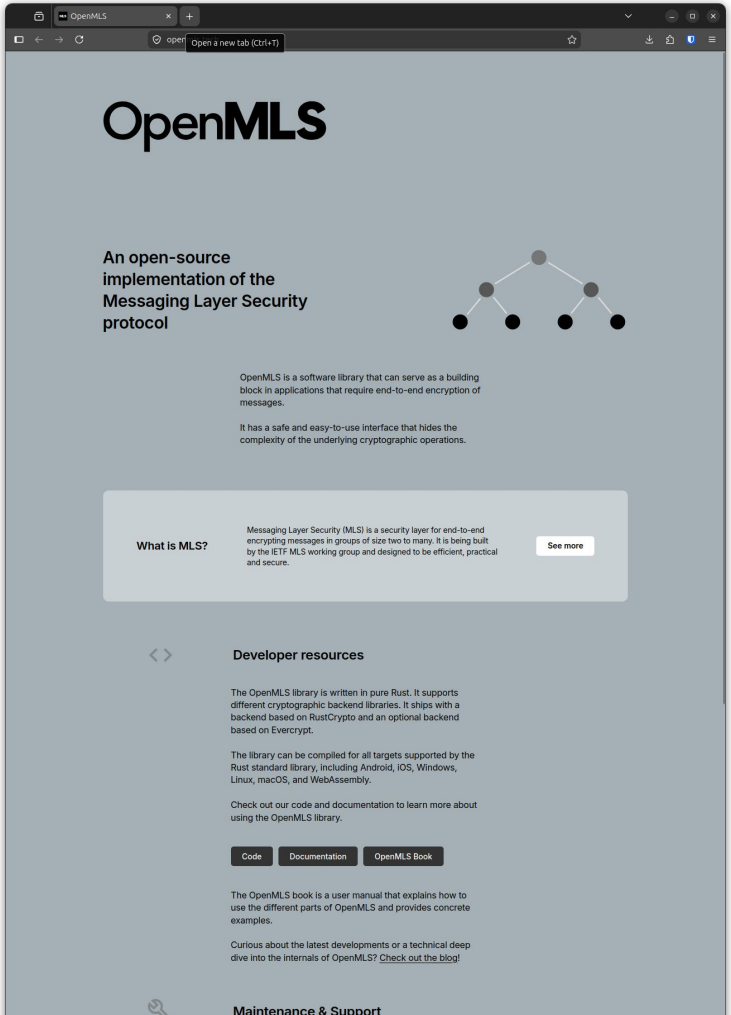


Ratchet tree update



OpenMLS

- Open-source Rust implementation of MLS
- Security audit published May 2026
- Maintainers very friendly and responsive
- Draft of post-quantum ciphersuite



Group messaging in Sentinel

Conversation Groups

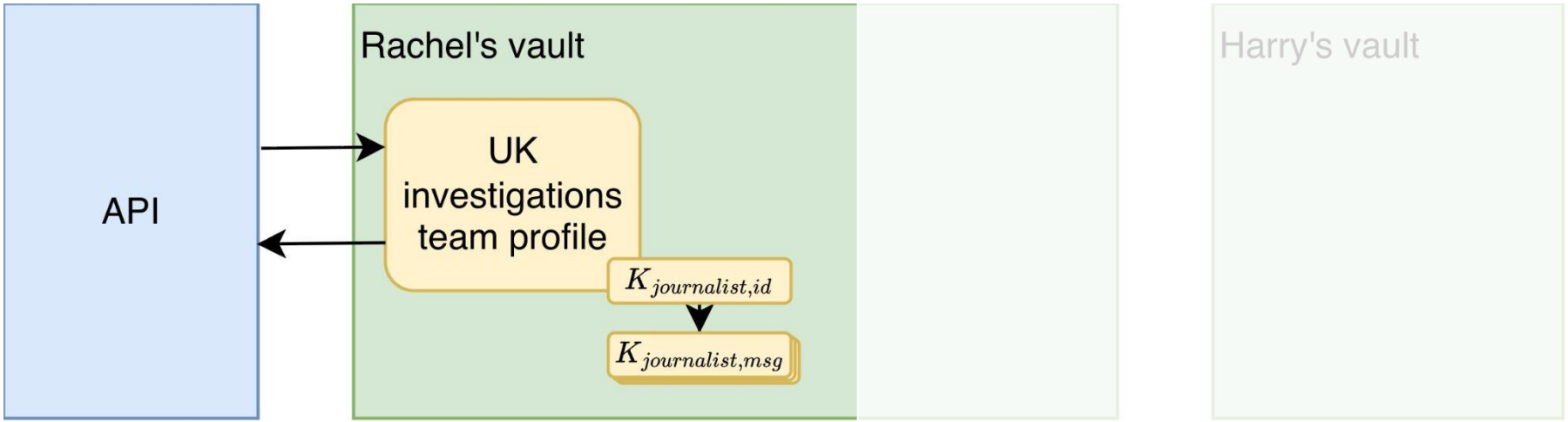
Allow Sentinel user to forward messages to & from sources

Shared Profile Groups

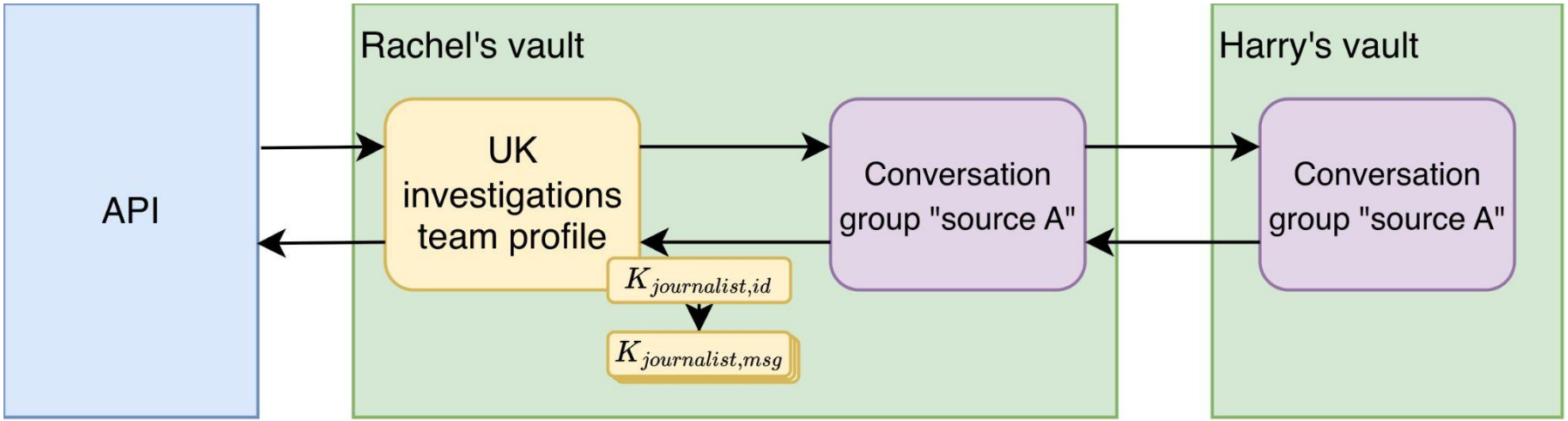
Allow multiple Sentinel users to share management of journalist profile.

Works by securely sharing private journalist keys

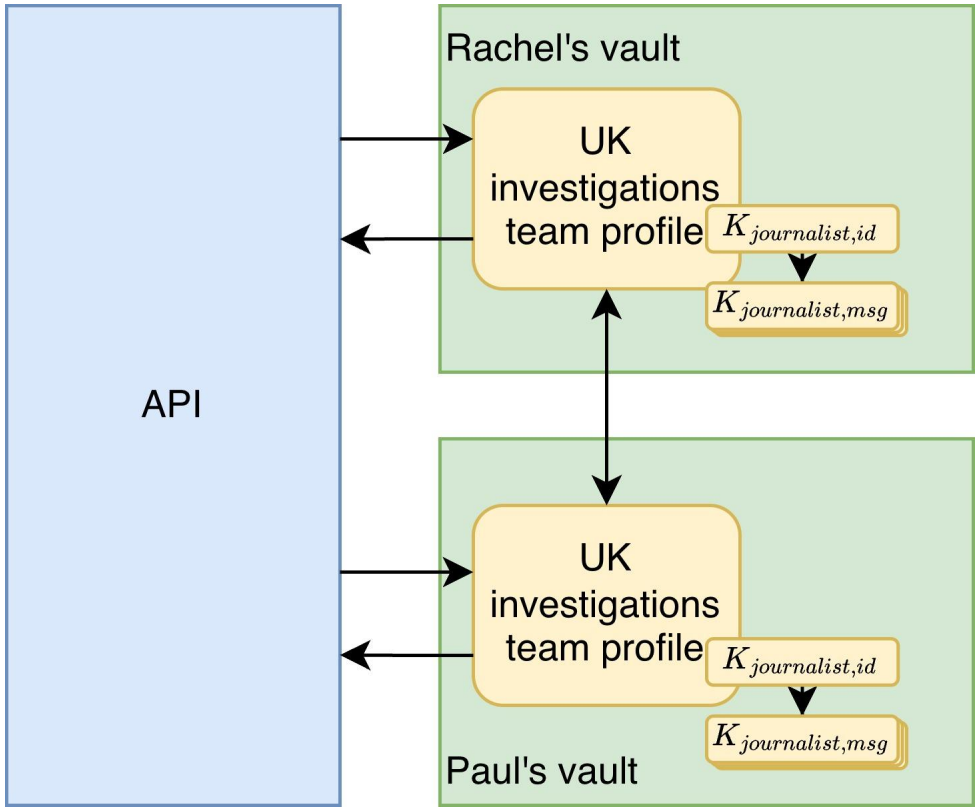
Message forwarding in **conversation groups**



Message forwarding in **conversation groups**



Keys synchronised in **shared profile groups**

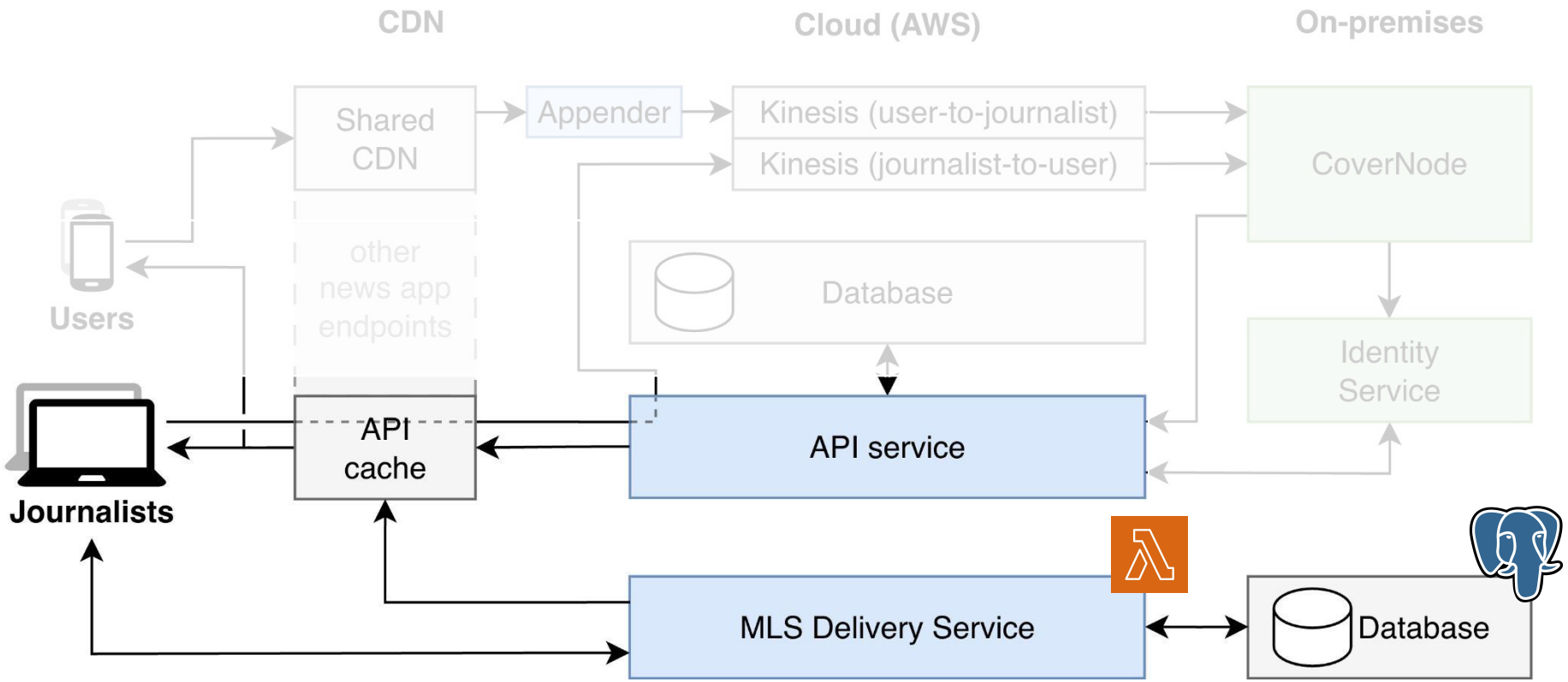


MLS Services

Delivery Service

- **Directory** that provides the initial keying material
- **Routes messages** between clients, acting as a message broadcaster
- Make sure that all clients agree on the **order of messages**
- Not assumed to be trusted

CoverDrop's MLS Delivery Service



MLS Services

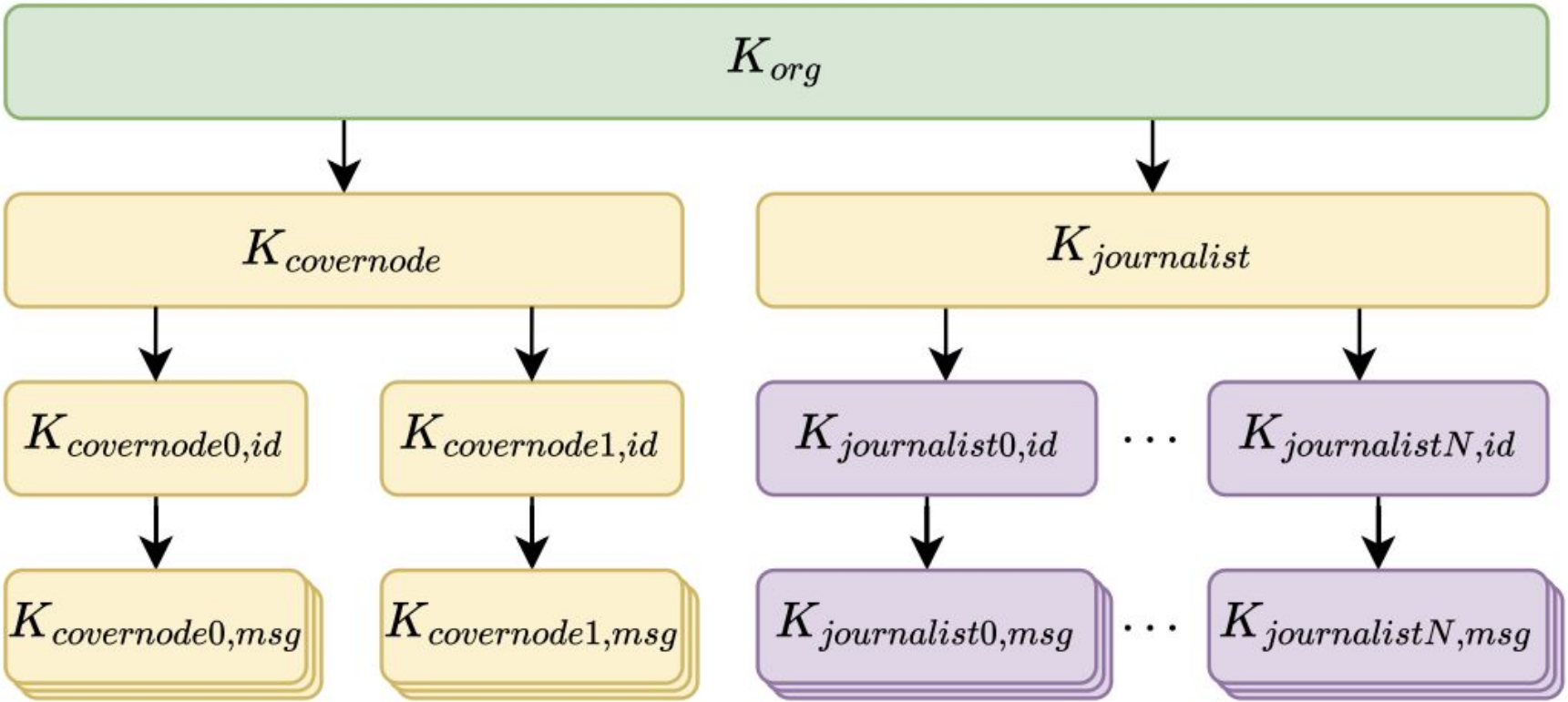
Delivery Service

- **Directory** that provides the initial keying material
- **Routes messages** between clients, acting as a message broadcaster
- Make sure that all clients agree on the **order of messages**
- Not assumed to be trusted

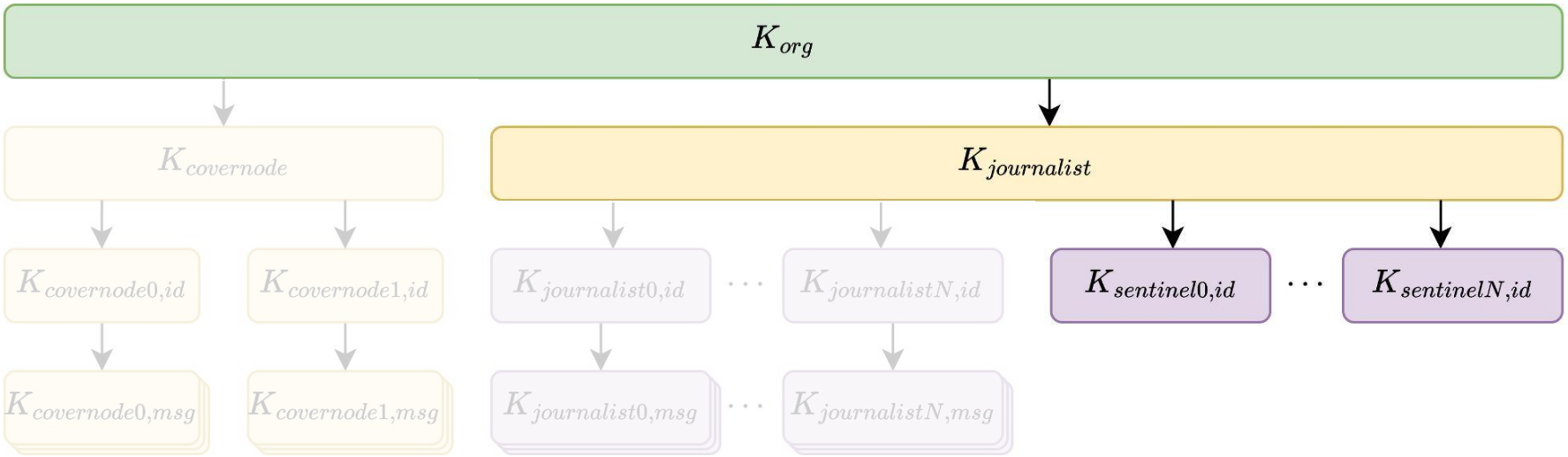
Authentication Service

- **Issue credentials** to clients
- Enables group members to **authenticate** the credentials presented by other group members
- **Trusted** - a malicious AS can allow an attacker to impersonate any client

Existing CoverDrop Authentication



CoverDrop's MLS Authentication Service



MLS Auth Service

- MLS client credential = **sentinel id**
- MLS client's signing key = **sentinel id key**

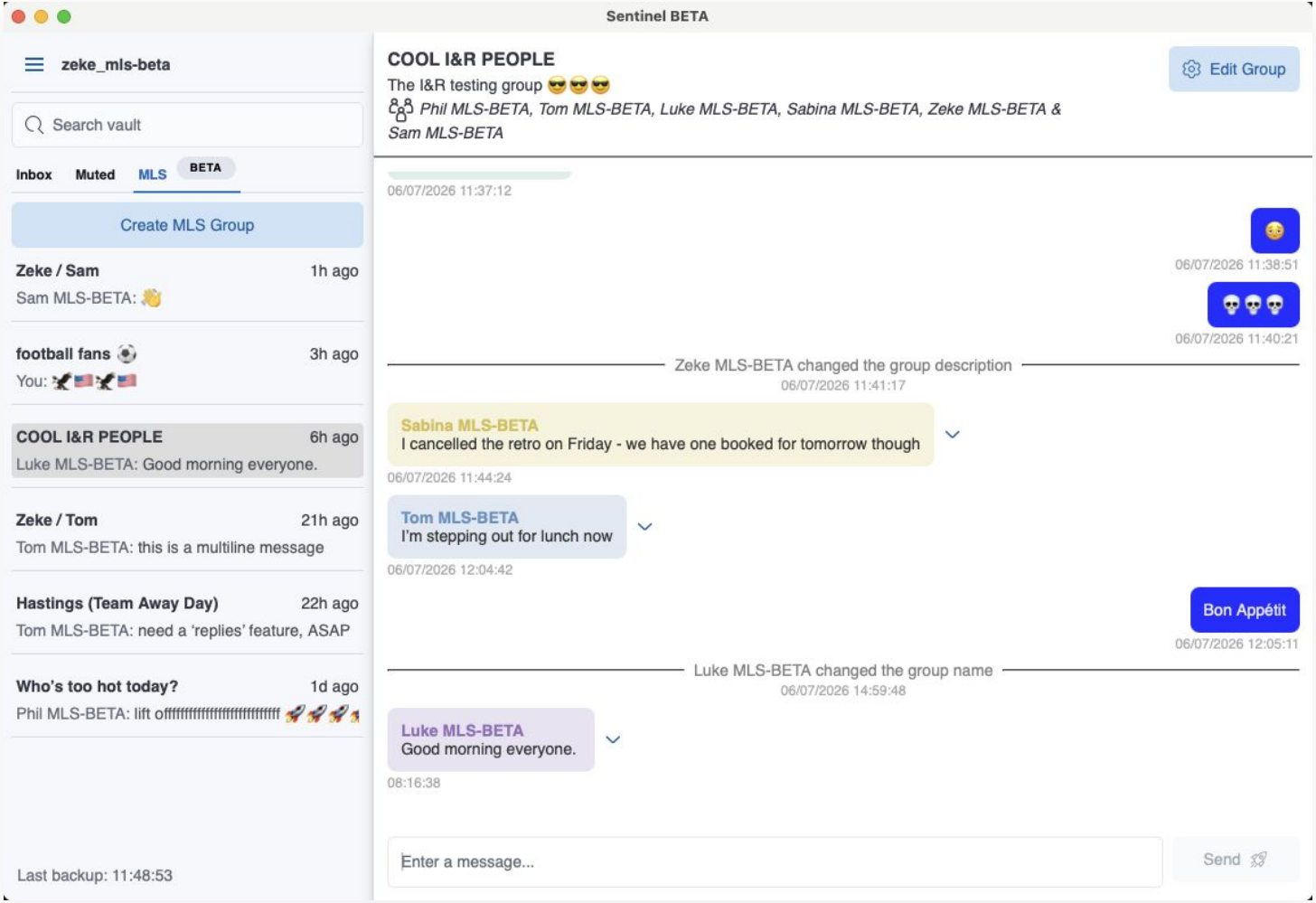
Response from API public-keys endpoint

OpenMLS ciphersuites

Ciphersuite	Security level in bits	KEM	AEAD algorithm	Hash algorithm	Signature algorithm
0x0001	128	DH KEM x25519	AES-GCM 128	SHA2-256	**Ed25519**
0x0002	128	DH KEM P256	AES-GCM 128	SHA2-256	EcDSA P256
0x0003	128	DH KEM x25519	Chacha20Poly1305	SHA2-256	**Ed25519**
0x0004	256	DH KEM x448	AES-GCM 256	SHA2-512	Ed448
0x0005	256	DH KEM P521	AES-GCM 256	SHA2-512	EcDSA P521
0x0006	256	DH KEM x448	Chacha20Poly1305	SHA2-512	Ed448
0x0007	256	DH KEM P384	AES-GCM 256	SHA2-384	EcDSA P384
0x004D	256	X-WING KEM draft-01	Chacha20Poly1305	SHA2-256	Ed25519

Group messaging roadmap

- ✅ **Experiment with OpenMLS**, create design, get feedback
- ✅ Create **MLS Delivery Service**
- ✅ Create **MLS Authentication Service**
- ⏳ Turn Sentinel into a group messaging client for testing
- 🤖 Shared **read-only access** to source conversations
- 🤖 Shared **read-write access** to source conversations
- 🤖 **Shared management** of journalist profiles


Sentinel BETA
zeke_mls-beta
Search vault
Inbox
Muted
MLS
BETA
Create MLS Group
Zeke / Sam
1h ago
Sam MLS-BETA: 👋
football fans ⚽
3h ago
You: 🦅🇺🇸🦅🇺🇸
COOL I&R PEOPLE
6h ago
Luke MLS-BETA: Good morning everyone.
Zeke / Tom
21h ago
Tom MLS-BETA: this is a multiline message
Hastings (Team Away Day)
22h ago
Tom MLS-BETA: need a 'replies' feature, ASAP
Who's too hot today?
1d ago
Phil MLS-BETA: lift offffffffffffffffffffffffffff 🚀🚀🚀
Last backup: 11:48:53
COOL I&R PEOPLE
The I&R testing group 😎😎😎
Phil MLS-BETA, Tom MLS-BETA, Luke MLS-BETA, Sabina MLS-BETA, Zeke MLS-BETA & Sam MLS-BETA
Edit Group
06/07/2026 11:37:12
06/07/2026 11:38:51
06/07/2026 11:40:21
Zeke MLS-BETA changed the group description
06/07/2026 11:41:17
Sabina MLS-BETA
I cancelled the retro on Friday - we have one booked for tomorrow though
06/07/2026 11:44:24
Tom MLS-BETA
I'm stepping out for lunch now
06/07/2026 12:04:42
Bon Appétit
06/07/2026 12:05:11
Luke MLS-BETA changed the group name
06/07/2026 14:59:48
Luke MLS-BETA
Good morning everyone.
08:16:38
Enter a message...
Send

MLS challenges

MLS spec is complex, very broad

AS + DS = relatively high barrier to entry

Complex state management across distributed system:
Partial failures, consensus, error handling, transactionality, …

Thank you!

Learn more: **coverdrop.org**
github.com/guardian/coverdrop

The original CoverDrop research team


Mansoor Ahmed


Daniel Hugenroth


Diana A. Vasile


Alastair R. Beresford


Ross Anderson

The Guardian crew and contributors


Sam Cutler


Luke Hoyland


Philip McMahon


Tom Richards


Zeke Hunter-Green


Sabina Bejasa-Dimmock


Marjan Kalanaki


Sam Hession


Dom Kendrick


Mario Savarese


Chloe Kirton

UNIVERSITY OF CAMBRIDGE
Department of Computer Science and Technology

The Guardian

NOKIA BELL LABS

OPEN TECHNOLOGY FUND