End-to-End Encrypted Collaborative Documents

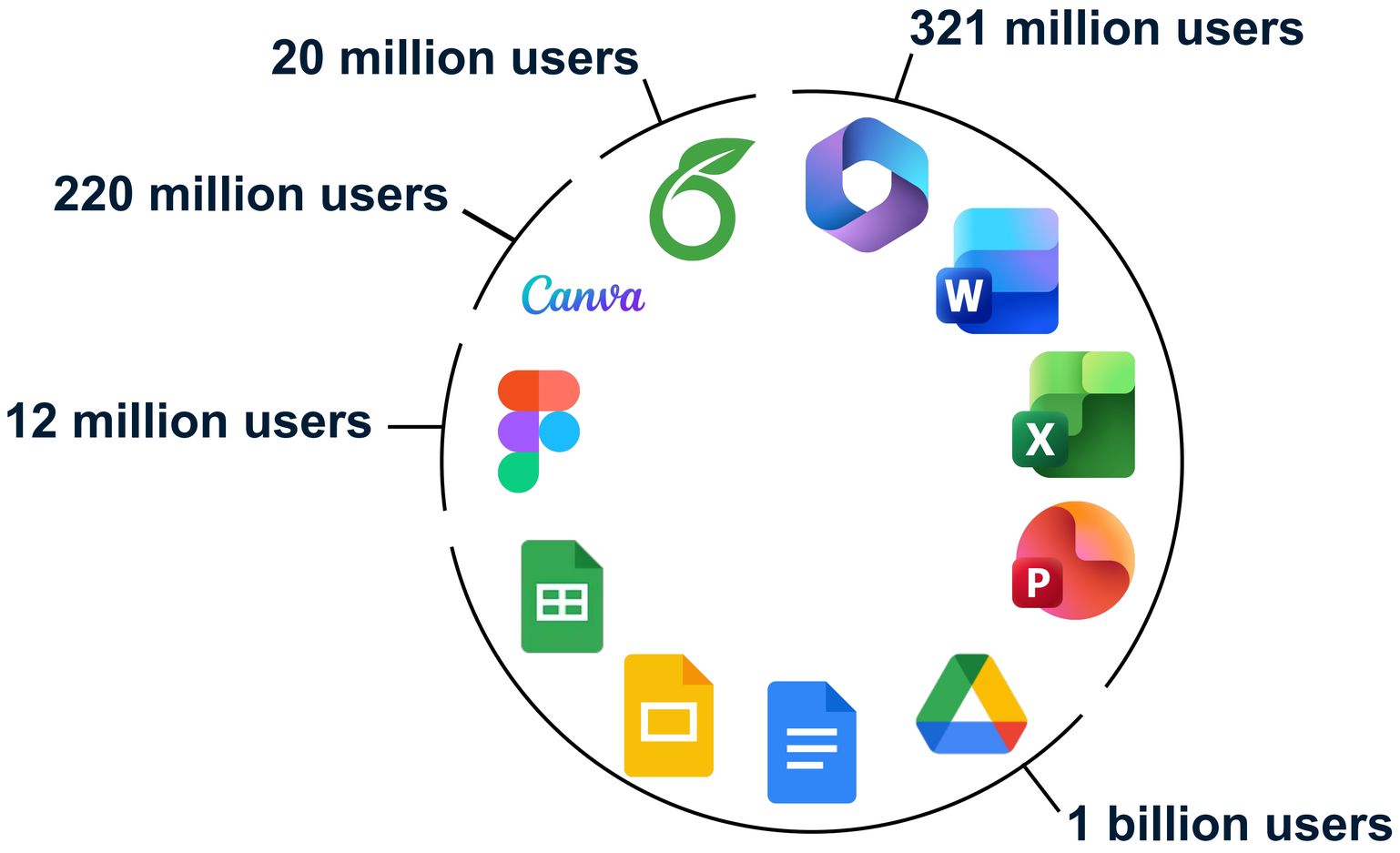
Christian Knabenhans* EPFL
Zayd Maradni* MPI-SP
Carmela Troncoso EPFL, MPI-SP
*these authors contributed equally to this work

USENIX Security'26

Collaborative documents



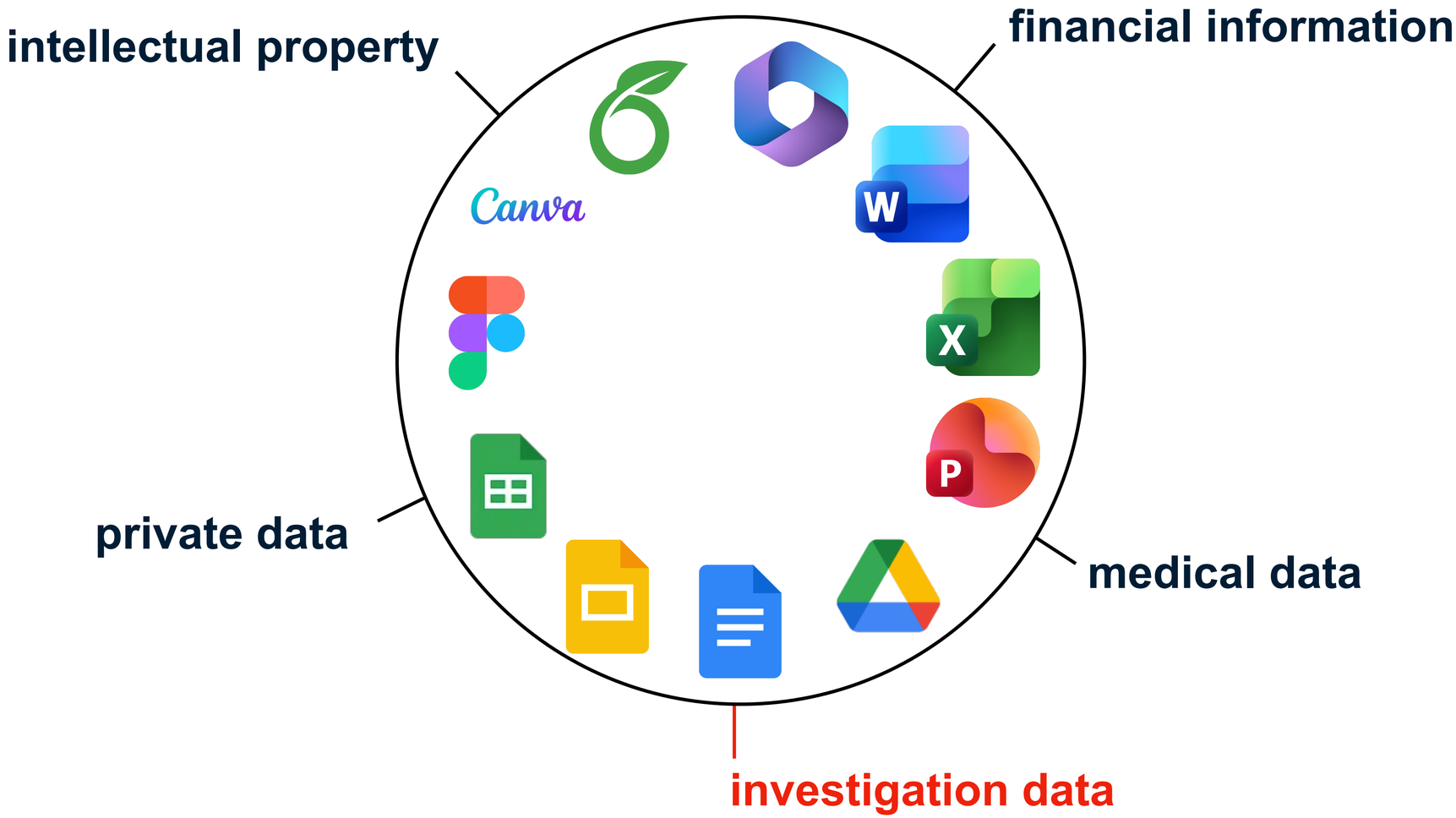
Collaborative documents are ubiquitous



Collaborative documents are sensitive



Collaborative documents are sensitive



Requirements of secure collaborative documents for investigative journalists

Requirements

with thanks to INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Requirements

with thanks to  INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Sharing docs

Requirements

with thanks to  INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Sharing docs

Collaboration

Requirements

with thanks to  INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Sharing docs

Collaboration

Convergence

Requirements

with thanks to  INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Sharing docs

Collaboration

Convergence

Asynchronous editing

Requirements

with thanks to  INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Sharing docs

Collaboration

Convergence

Asynchronous editing

Synchronous editing

Requirements

with thanks to  INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Sharing docs

Collaboration

Convergence

Asynchronous editing

Synchronous editing

Deployment

Requirements

with thanks to  INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Sharing docs

Collaboration

Convergence

Asynchronous editing

Synchronous editing

Deployment

No new accounts

Requirements

with thanks to  INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Sharing docs

Collaboration

Convergence

Asynchronous editing

Synchronous editing

Deployment

No new accounts

No new trust assumptions

Requirements

with thanks to  INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Sharing docs

Collaboration

Convergence

Asynchronous editing

Synchronous editing

Deployment

No new accounts

No new trust assumptions

No self-hosting

Requirements

with thanks to  INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Sharing docs

Collaboration

Convergence

Asynchronous editing

Synchronous editing

Deployment

No new accounts

No new trust assumptions

No self-hosting

can assume (untrusted) helper server

Requirements

with thanks to  INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Sharing docs

Collaboration

Convergence

Asynchronous editing

Synchronous editing

Deployment

No new accounts

No new trust assumptions

No self-hosting

can assume (untrusted) helper server

Security

Requirements

with thanks to  INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Sharing docs

Collaboration

Convergence

Asynchronous editing

Synchronous editing

Deployment

No new accounts

No new trust assumptions

No self-hosting

can assume (untrusted) helper server

Security

Confidentiality

Integrity

} E2EE

Requirements

with thanks to  INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Sharing docs

Collaboration

Convergence

Asynchronous editing

Synchronous editing

Deployment

No new accounts

No new trust assumptions

No self-hosting

can assume (untrusted) helper server

Security

Confidentiality

Integrity

} E2EE

Access control (read/comment/write/admin)

Requirements

with thanks to  INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Sharing docs

Collaboration

Convergence

Asynchronous editing

Synchronous editing

Deployment

No new accounts

No new trust assumptions

No self-hosting

can assume (untrusted) helper server

Security

Confidentiality } E2EE

Integrity

Access control (read/comment/write/admin)

Archiving

Requirements

with thanks to  INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Sharing docs

Collaboration

Convergence

Asynchronous editing

Synchronous editing

Deployment

No new accounts

No new trust assumptions

No self-hosting

can assume (untrusted) helper server

Security

Confidentiality

Integrity

} E2EE

Access control (read/comment/write/admin)

Archiving

Deleting

Requirements

with thanks to  INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Functional

Sharing docs

Collaboration

Convergence

Asynchronous editing

Synchronous editing

Deployment

No new accounts

No new trust assumptions

No self-hosting

can assume (untrusted) helper server

Security

Confidentiality

Integrity

} E2EE

Access control (read/comment/write/admin)

Archiving

Deleting

against malicious server

Existing secure collaborative docs

Existing secure collaborative docs

	satisfies functional reqs.	satisfies deployment reqs.	(provably) satisfies security reqs.
Academic Capsule [Kob18] SnapDoc [KKB19] HE/MPC [BFMPP21,PPJP23]	~	✗	✓

[Kob18] Kobeissi, “Capsule: A Protocol for Secure Collaborative Document Editing”, ePrint’18
[KKB19] Kollmann, Kleppmann, Beresford, “Snapdoc: Authenticated snapshots with history privacy in peer-to-peer collaborative editing”, PETS’19
[BFMPP21] Barbosa, Ferreira, Marques, Portela, Preguiça, “Secure conflict-free replicated data types”, ICDCN’21
[PPJP23] Portela, Pacheco, Jorge, Pontes, “General-purpose secure conflict-free replicated data types”, CSF’23

Existing secure collaborative docs

	satisfies functional reqs.	satisfies deployment reqs.	(provably) satisfies security reqs.
Academic Capsule [Kob18] SnapDoc [KKB19] HE/MPC [BFMPP21,PPJP23]	~	✗	✓
Deployed CryptPad Apple Notes* ProtonDocs	✓	✗	~

[Kob18] Kobeissi, “Capsule: A Protocol for Secure Collaborative Document Editing”, ePrint’18
[KKB19] Kollmann, Kleppmann, Beresford, “Snapdoc: Authenticated snapshots with history privacy in peer-to-peer collaborative editing”, PETS’19
[BFMPP21] Barbosa, Ferreira, Marques, Portela, Preguiça, “Secure conflict-free replicated data types”, ICDCN’21
[PPJP23] Portela, Pacheco, Jorge, Pontes, “General-purpose secure conflict-free replicated data types”, CSF’23

Existing secure collaborative docs

	satisfies functional reqs.	satisfies deployment reqs.	(provably) satisfies security reqs.
Academic Capsule [Kob18] SnapDoc [KKB19] HE/MPC [BFMPP21,PPJP23]	~	✗	✓
Deployed CryptPad Apple Notes* ProtonDocs	✓	✗	~

Also: E2EE cloud storage, E2EE Git

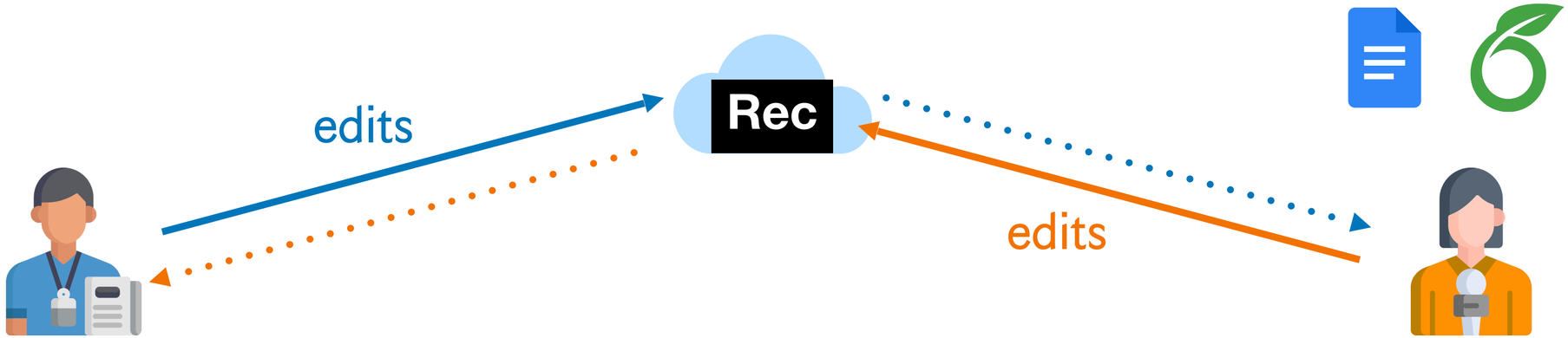
[Kob18] Kobeissi, “Capsule: A Protocol for Secure Collaborative Document Editing”, ePrint’18
[KKB19] Kollmann, Kleppmann, Beresford, “Snapdoc: Authenticated snapshots with history privacy in peer-to-peer collaborative editing”, PETS’19
[BFMPP21] Barbosa, Ferreira, Marques, Portela, Preguiça, “Secure conflict-free replicated data types”, ICDCN’21
[PPJP23] Portela, Pacheco, Jorge, Pontes, “General-purpose secure conflict-free replicated data types”, CSF’23

Building secure collaborative documents

Collaborative documents

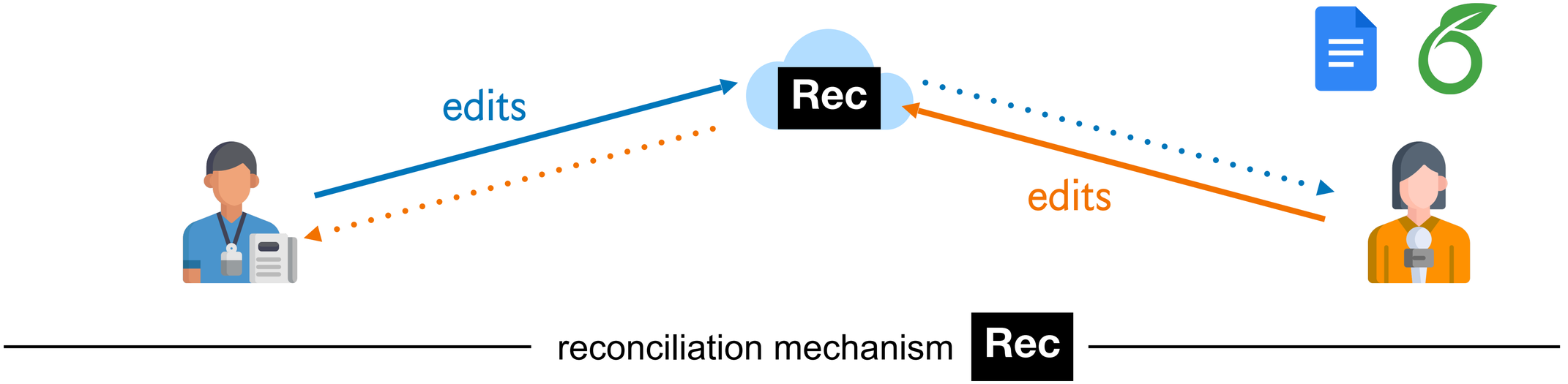
reconciliation mechanism **Rec**

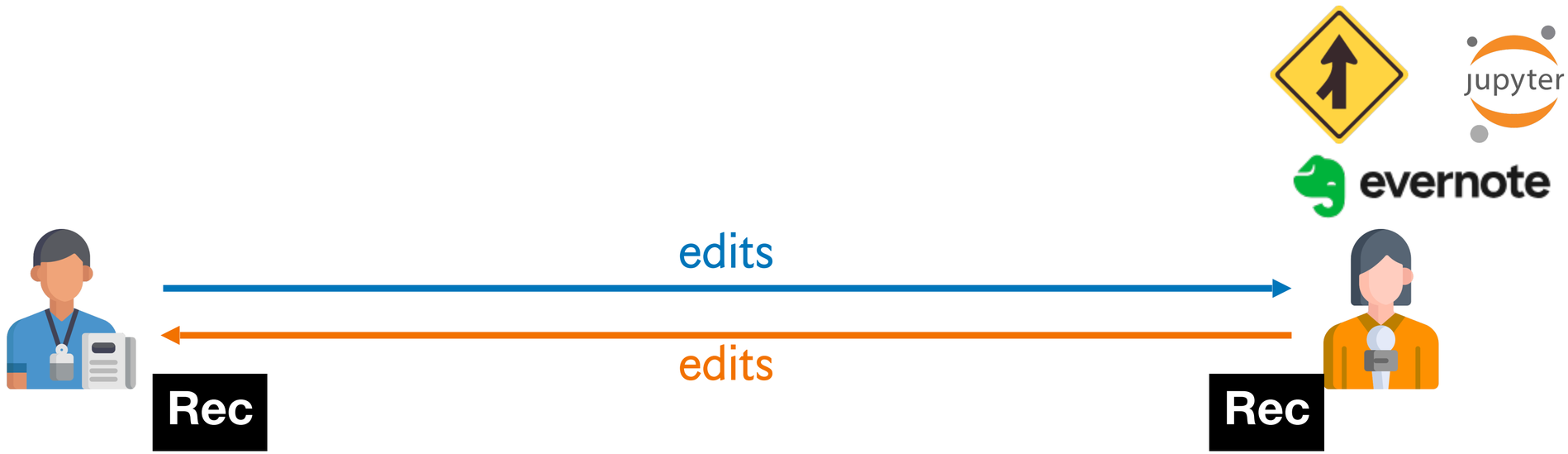
Collaborative documents



reconciliation mechanism **Rec**

Collaborative documents



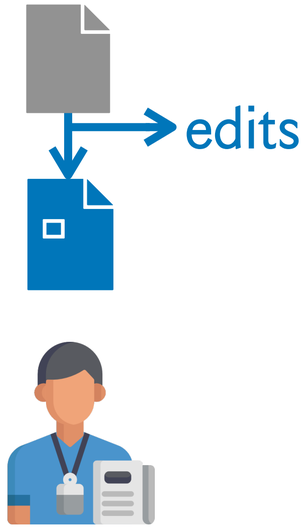


Reconciliation mechanism

Users receiving the same set of edits, regardless of order,
have the same view of the document

Reconciliation mechanism

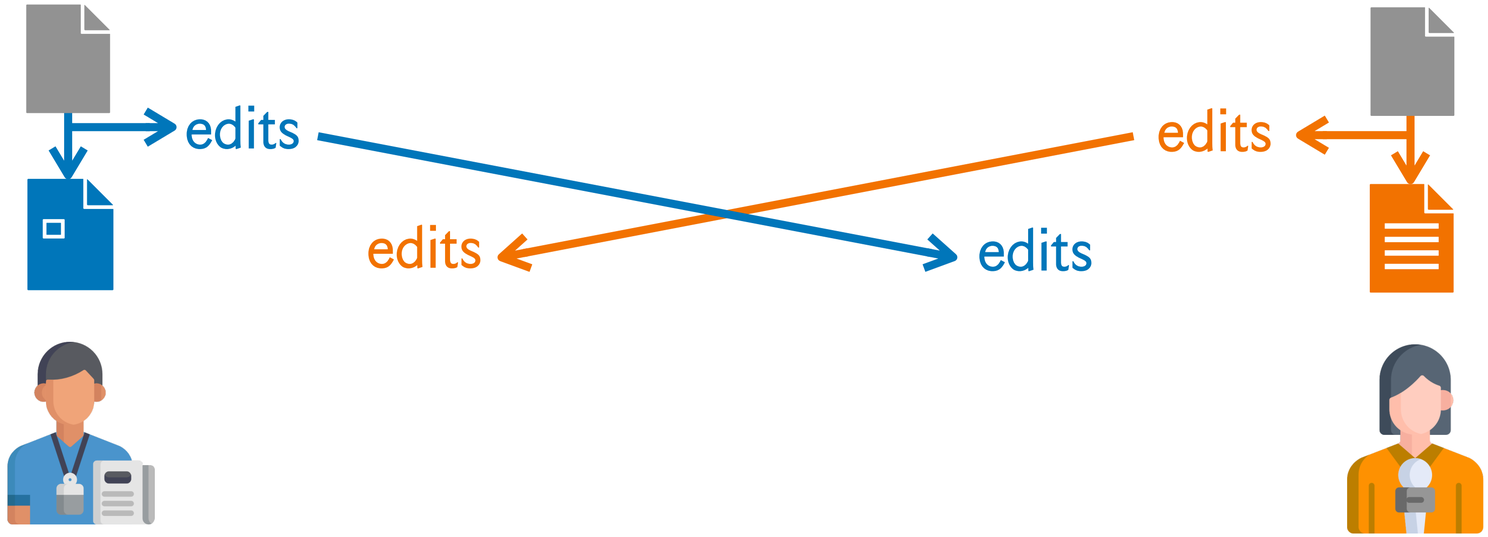
Users receiving the same set of edits, regardless of order, have the same view of the document





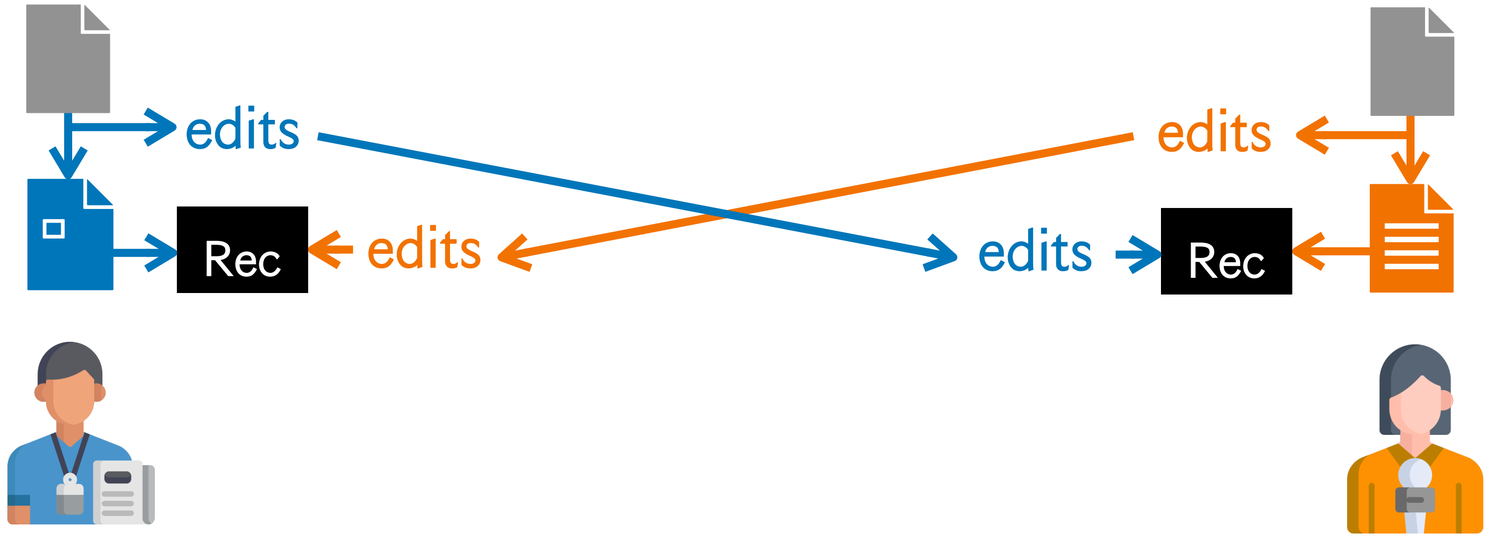
Reconciliation mechanism

Users receiving the same set of edits, regardless of order,
have the same view of the document



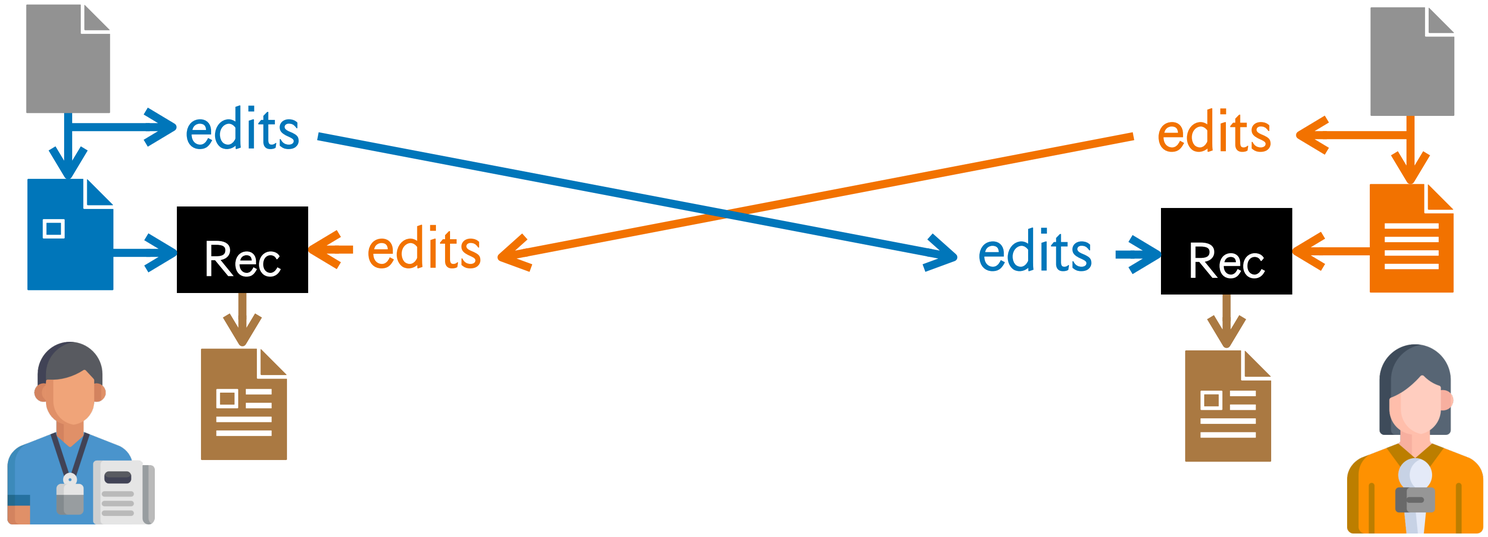
Reconciliation mechanism

Users receiving the same set of edits, regardless of order, have the same view of the document

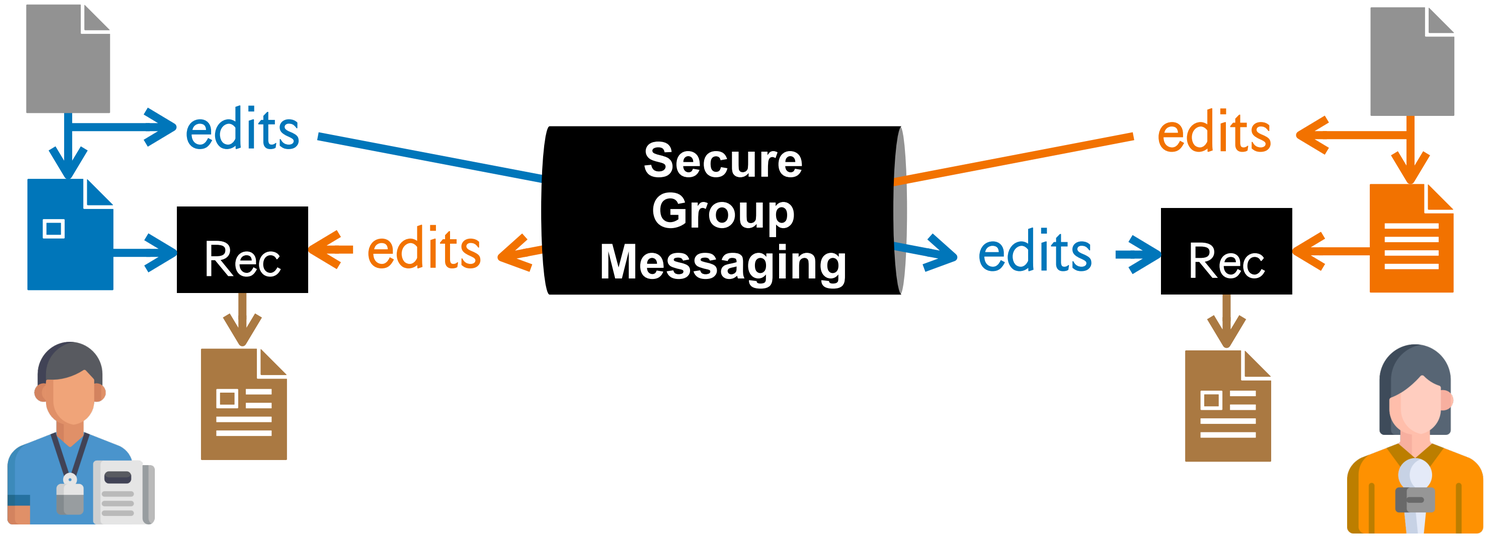


Reconciliation mechanism

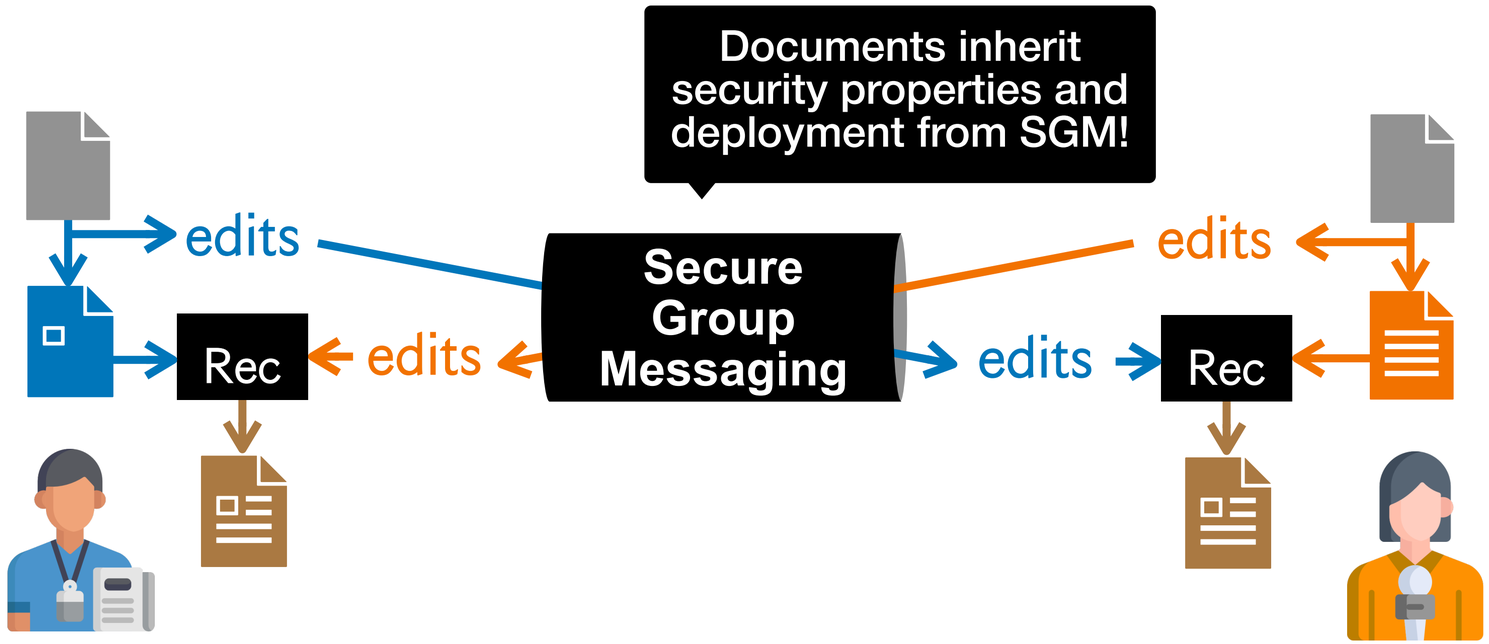
Users receiving the same set of edits, regardless of order, have the same view of the document



Secure Group Messaging is sufficient for E2EE CD



Secure Group Messaging is sufficient for E2EE CD



E2EE CD

Setup

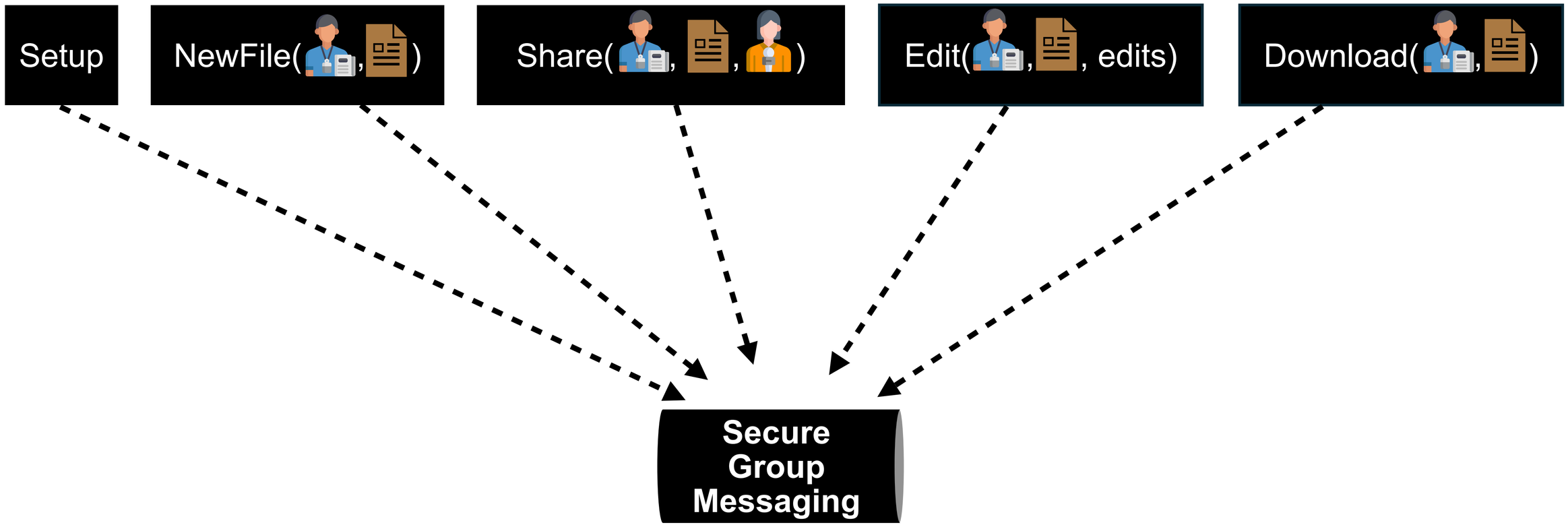
NewFile()

Share()

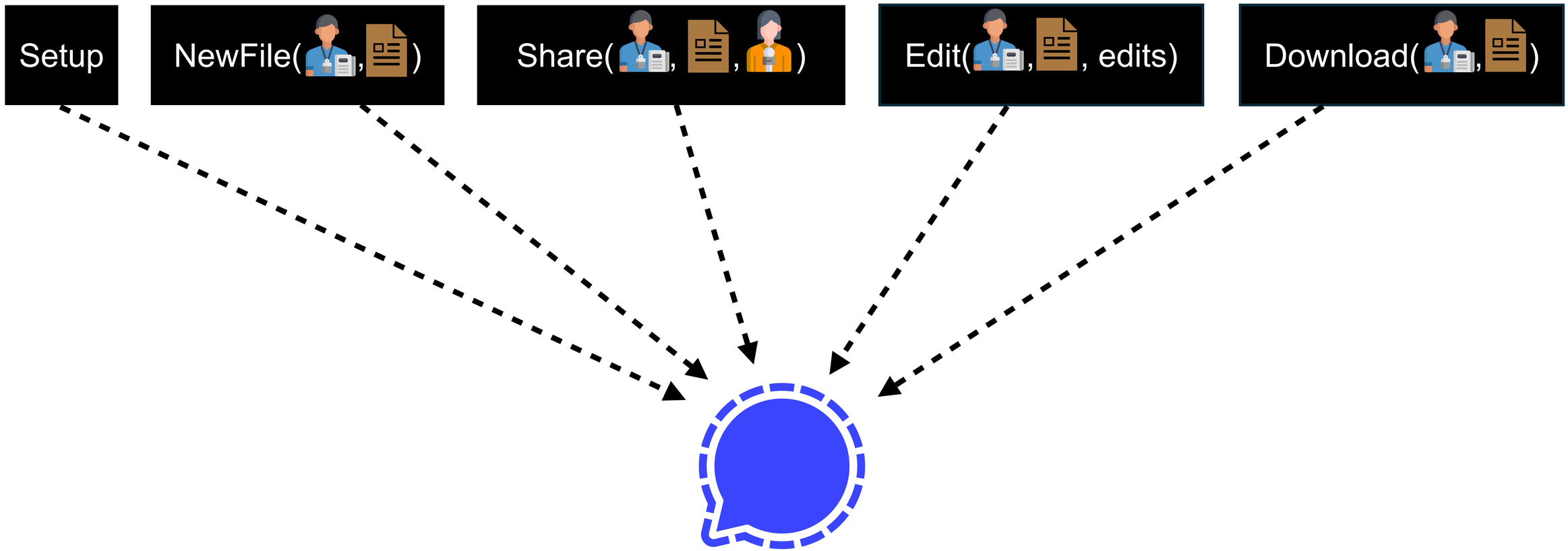
Edit(, edits)

Download()

E2EE CD


Setup
NewFile(,)
Share(, ,)
Edit(, , edits)
Download(,)
Secure Group Messaging

E2EE CD



E2EE CD from Signal

Setup | NewFile() | Share() | Edit( , edits) | Download()

Setup

Setup: link account



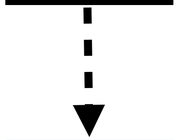
Signal user



SignalCD

E2EE CD from Signal

Setup



Setup

NewFile()

Share()

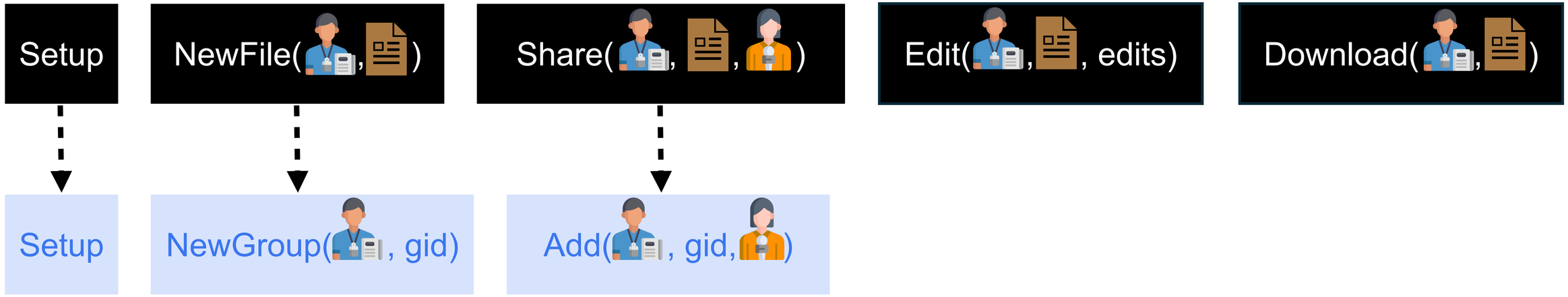
Edit( , edits)

Download()

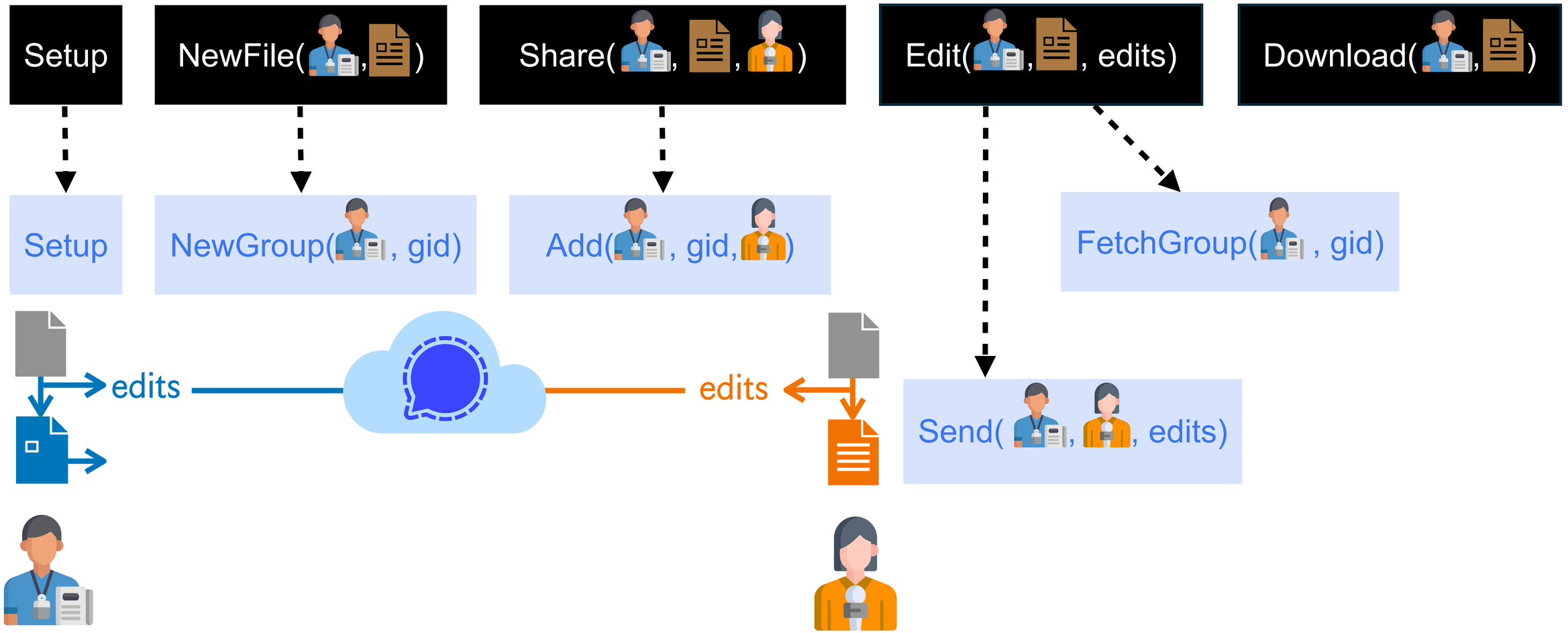
E2EE CD from Signal



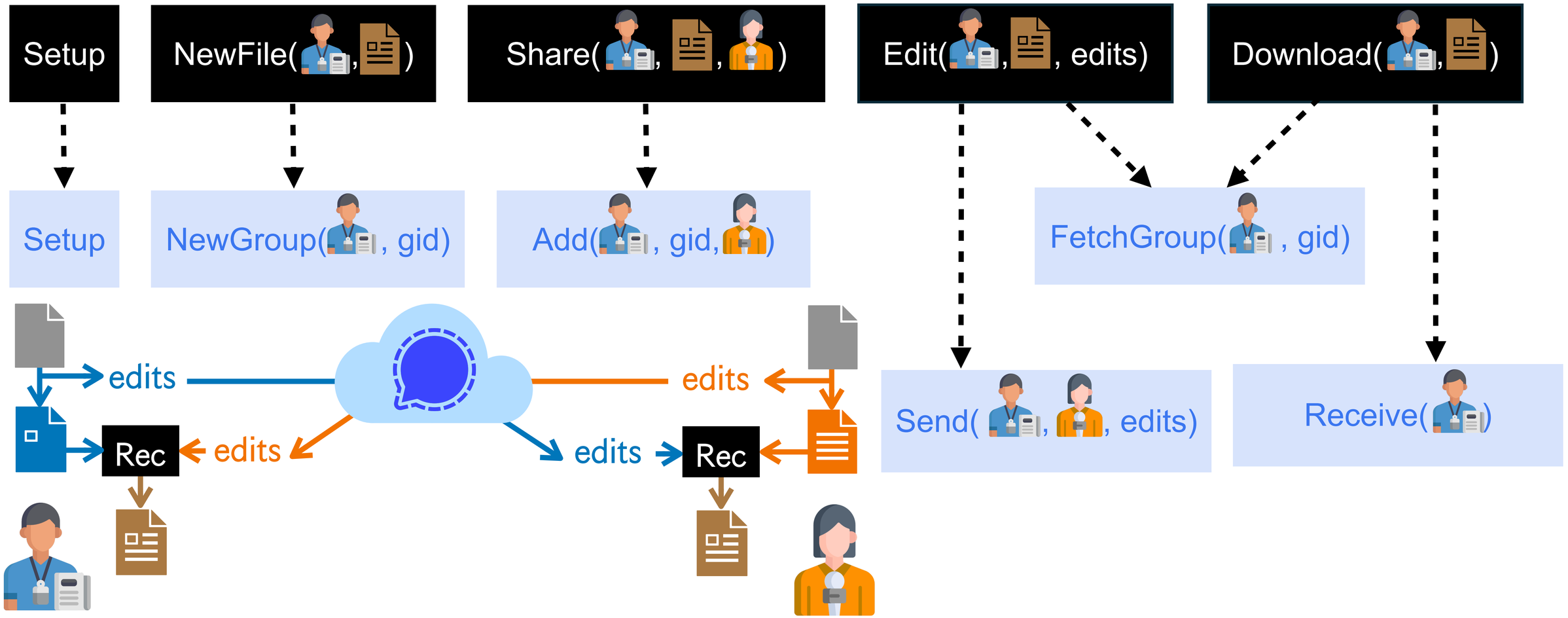
E2EE CD from Signal



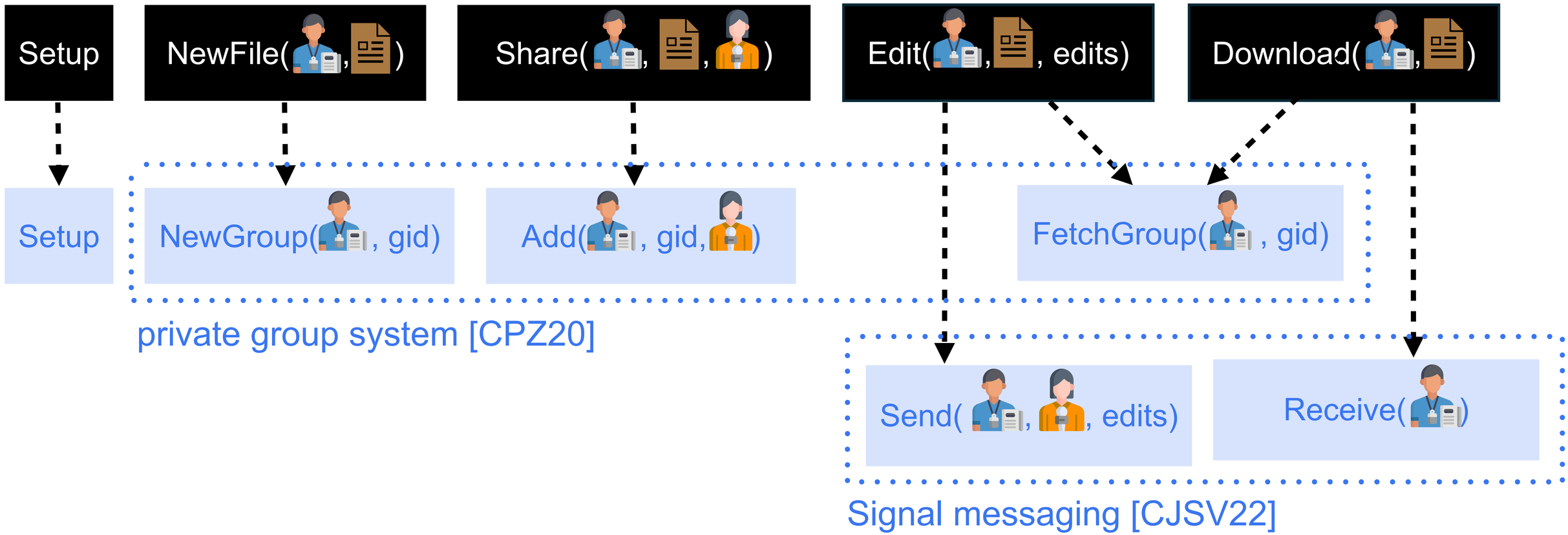
E2EE CD from Signal



E2EE CD from Signal



E2EE CD from Signal

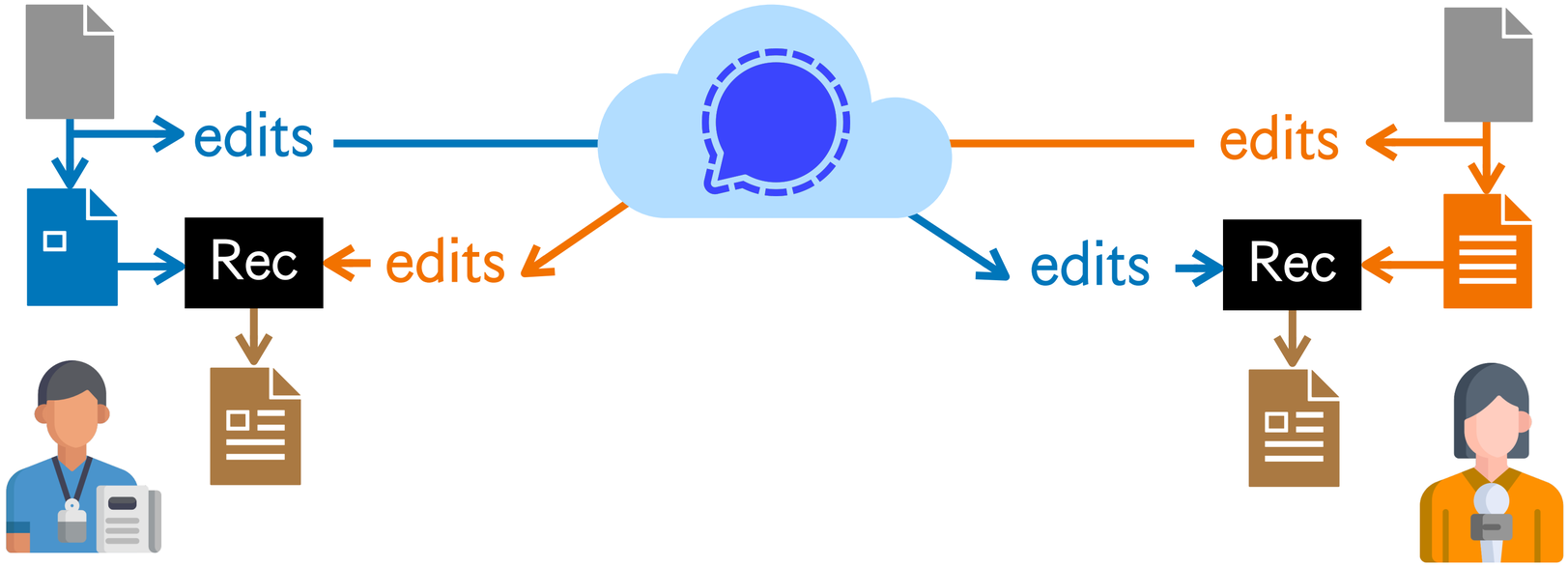


[CPZ20] Chase, Perrin, Zaverucha, “The Signal Private Group System and Anonymous Credentials Supporting Efficient Verifiable Encryption”, CCS’20
[CJSV22] Canetti, Jain, Swanberg, and Varia, “Universally Composable End-to-End Secure Messaging”, CRYPTO’22

Evaluation

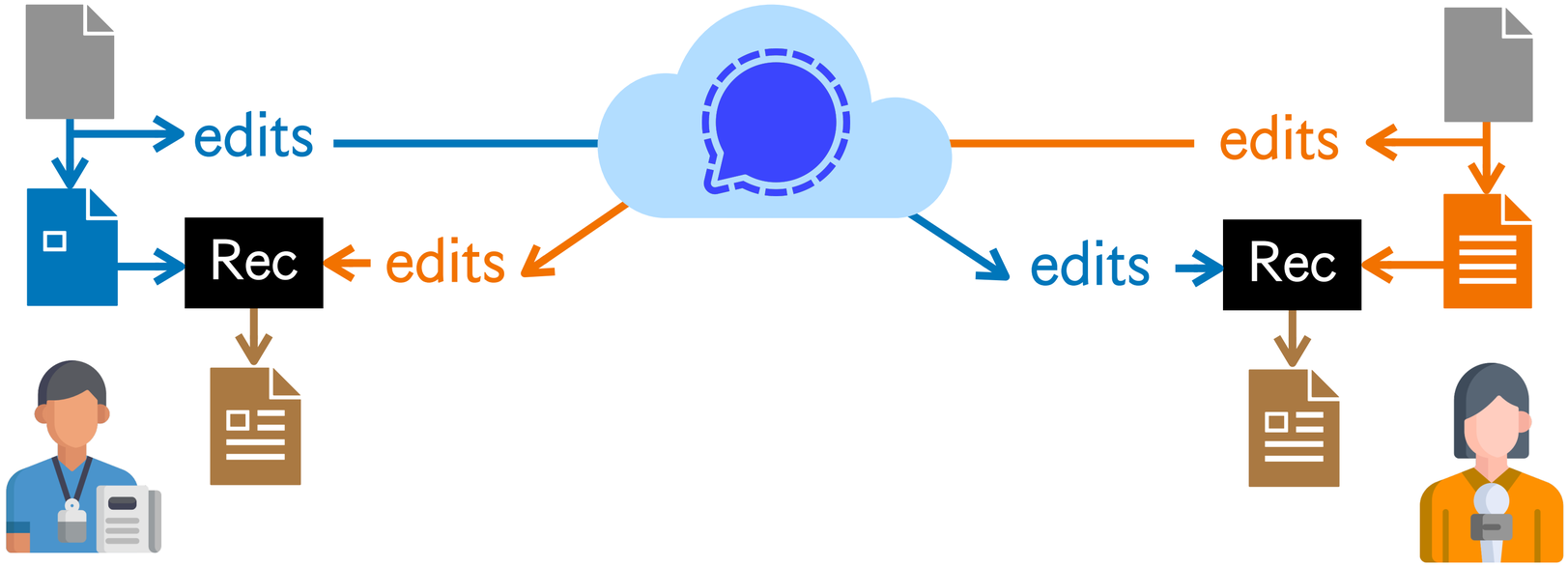
Evaluation setup

Edit: apply locally, send encrypted edit, reconcile



Evaluation setup

Edit: apply locally, send encrypted edit, reconcile



types at 40–60 wpm

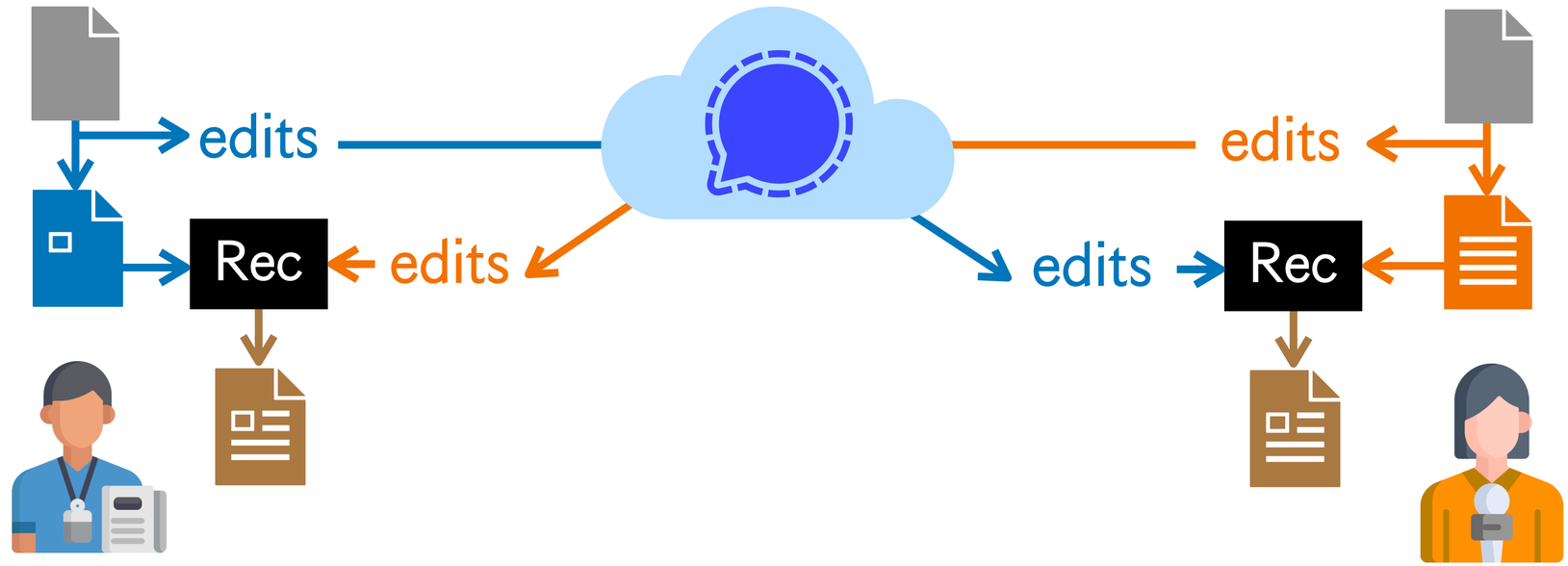
types at 30–120 wpm

Evaluation setup

slow: out-of-office / 4G (5 Mbits/s, 30ms latency)

fast: in-office / wifi (60 Mbits/s, 5ms latency)

Edit: apply locally, send encrypted edit, reconcile



types at 40–60 wpm

types at 30–120 wpm

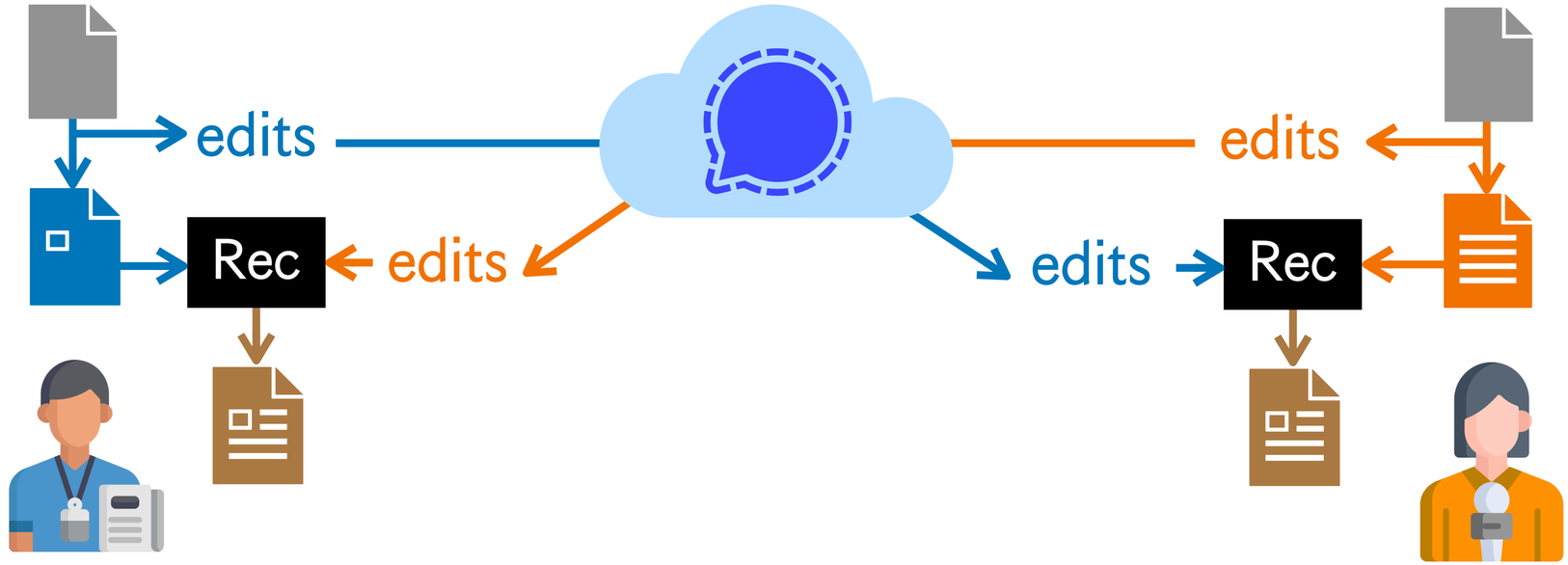
Evaluation setup

slow: out-of-office / 4G (5 Mbits/s, 30ms latency)

fast: in-office / wifi (60 Mbits/s, 5ms latency)

} network dominates → **single-character** edits

Edit: apply locally, send encrypted edit, reconcile



types at 40–60 wpm

types at 30–120 wpm

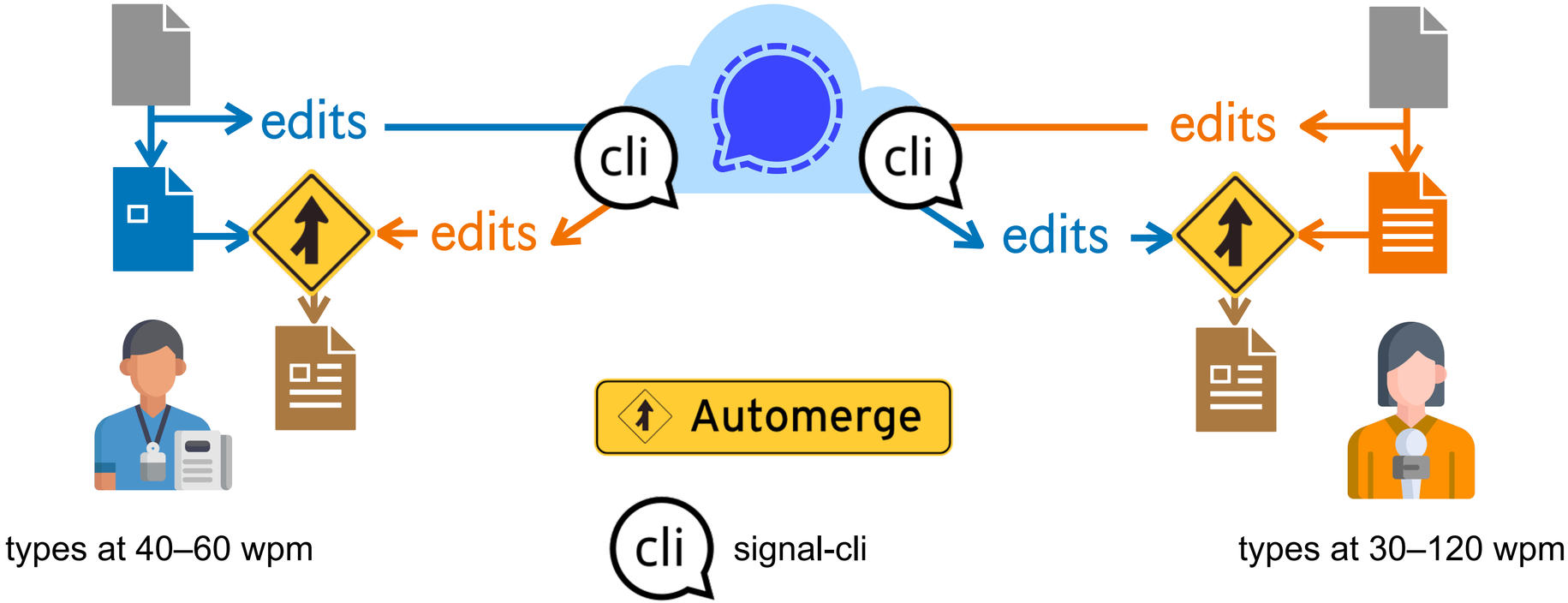
Evaluation setup

slow: out-of-office / 4G (5 Mbits/s, 30ms latency)

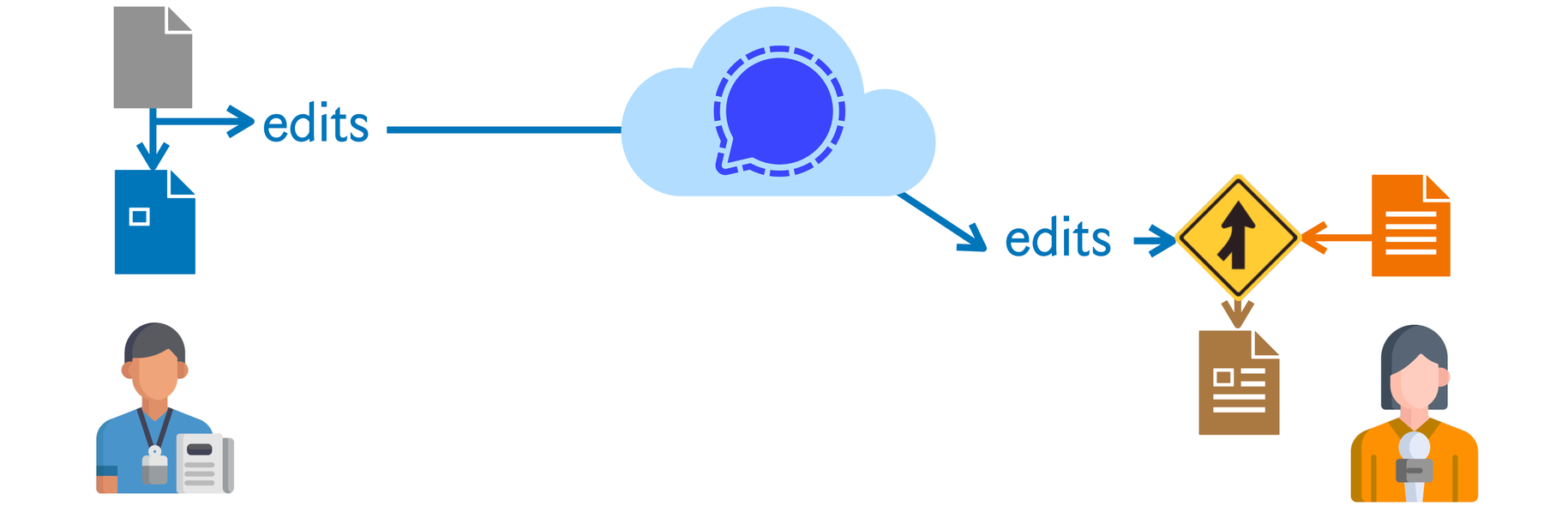
fast: in-office / wifi (60 Mbits/s, 5ms latency)

} network dominates → **single-character** edits

Edit: apply locally, send encrypted edit, reconcile



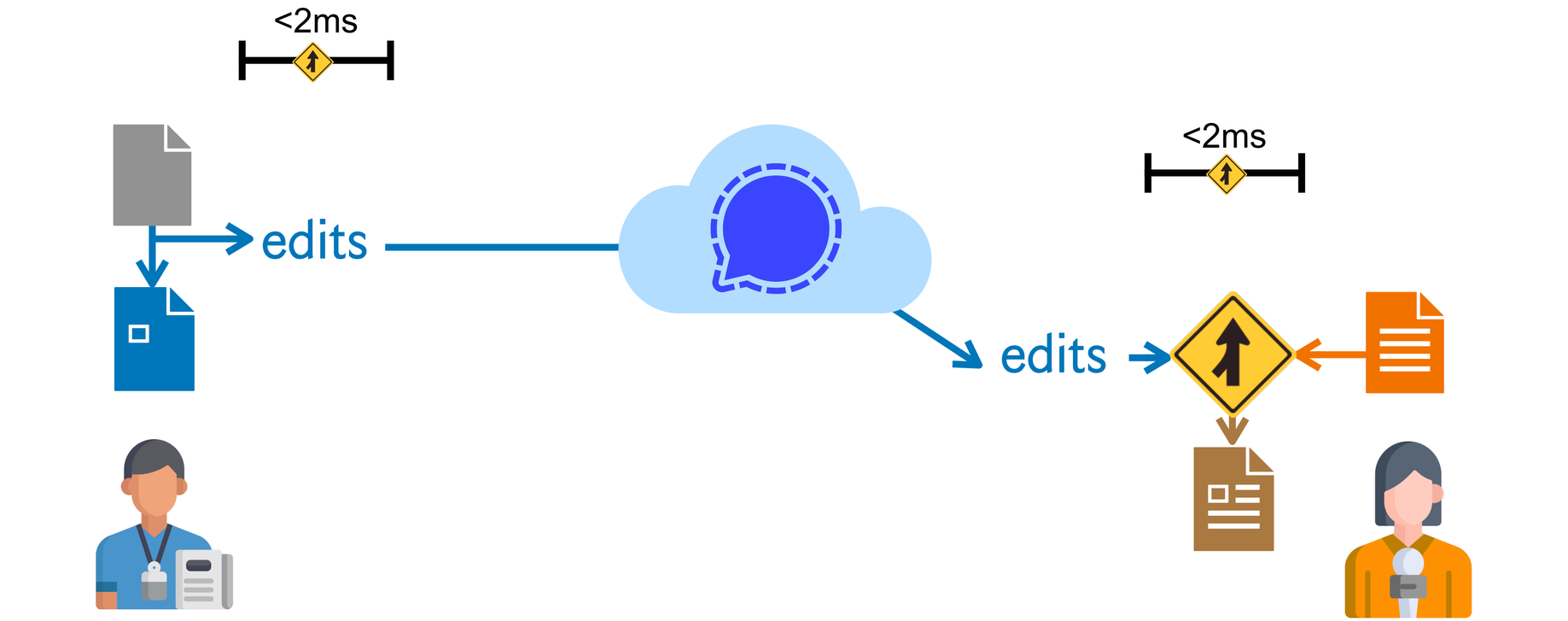
Synchronous editing



types at 40–60 wpm

types at 30–120 wpm

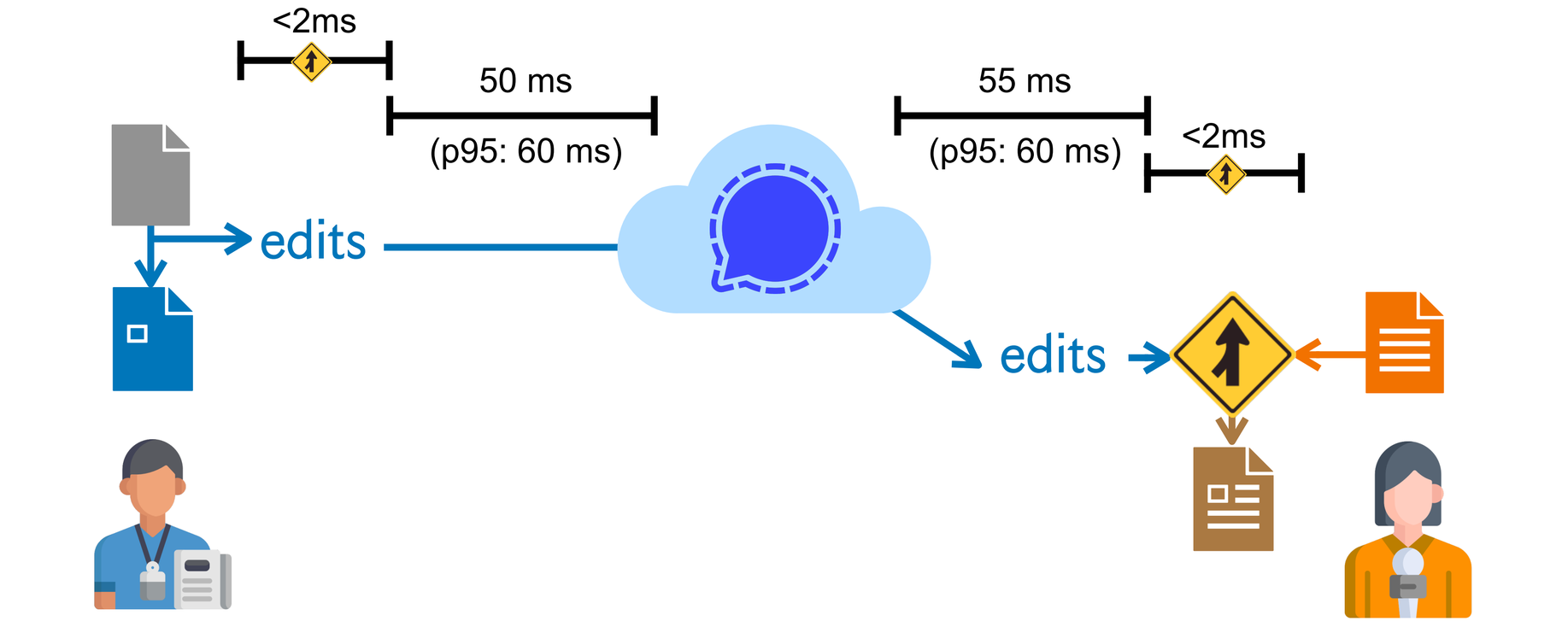
Synchronous editing



types at 40–60 wpm

types at 30–120 wpm

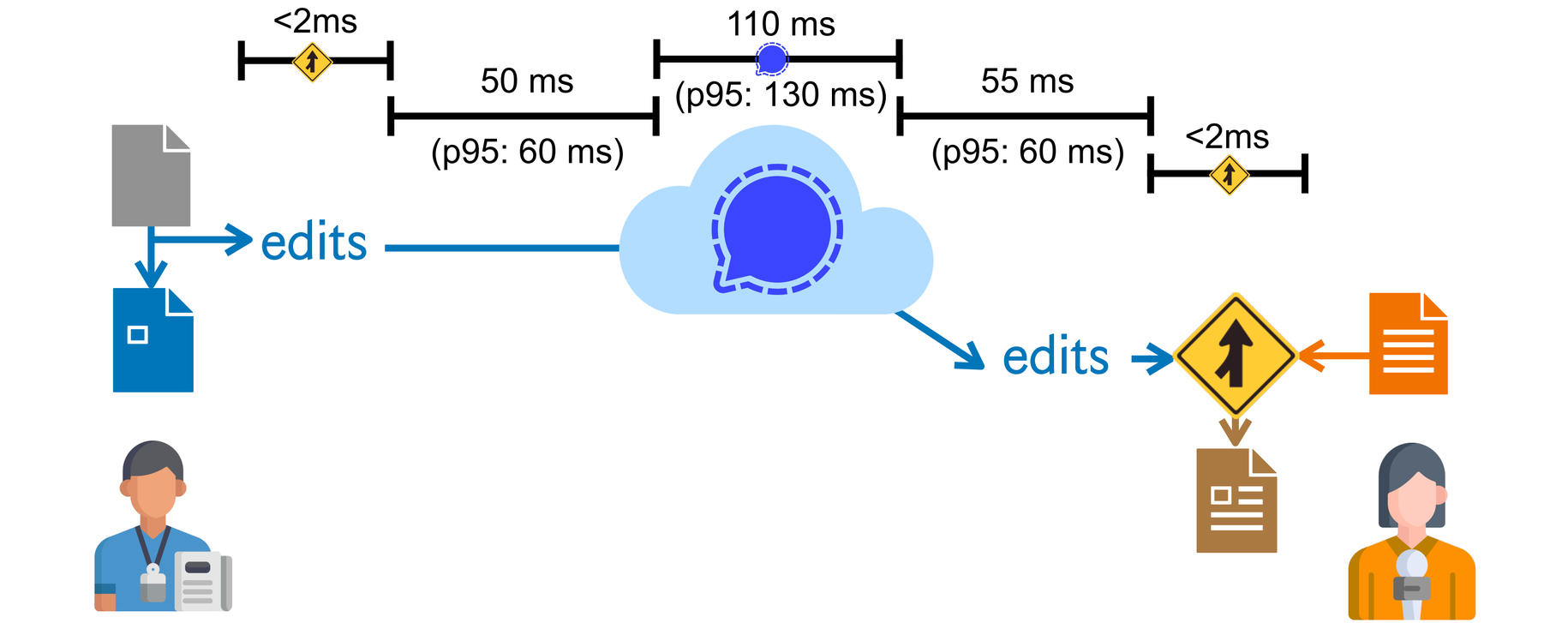
Synchronous editing



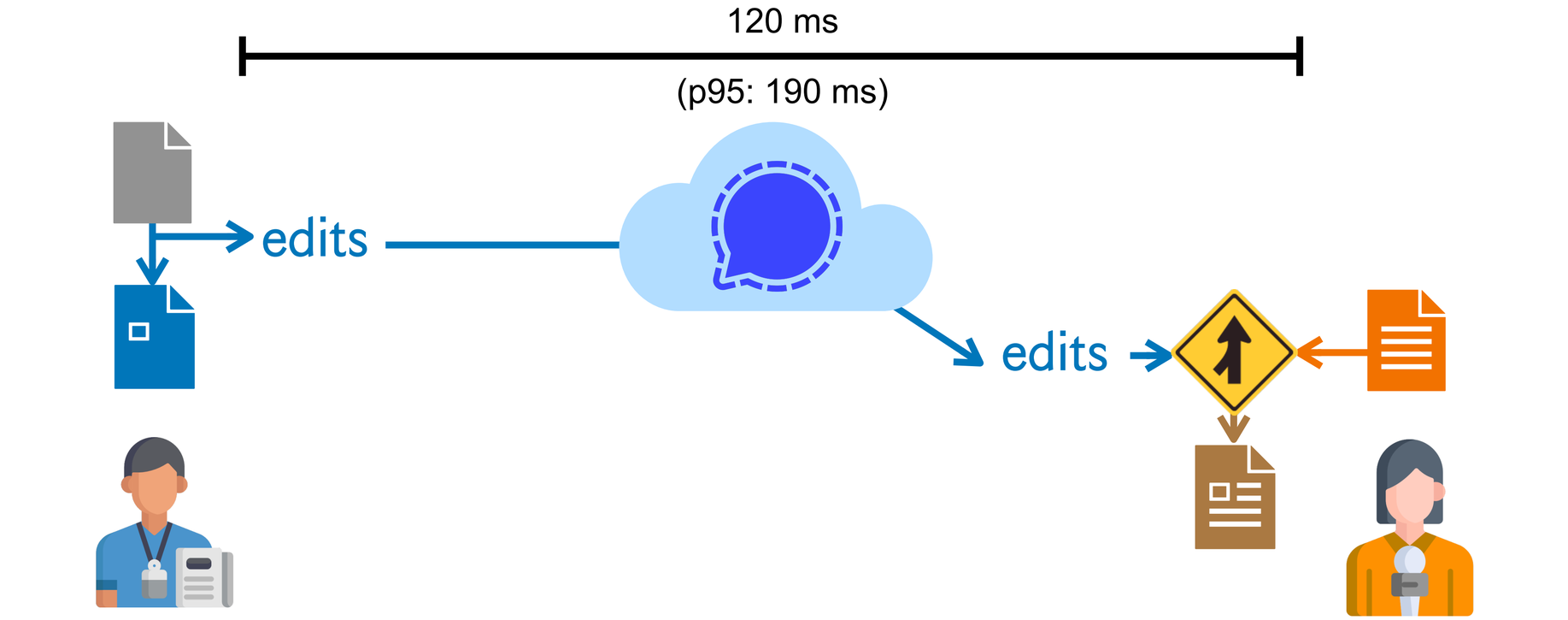
types at 40–60 wpm

types at 30–120 wpm

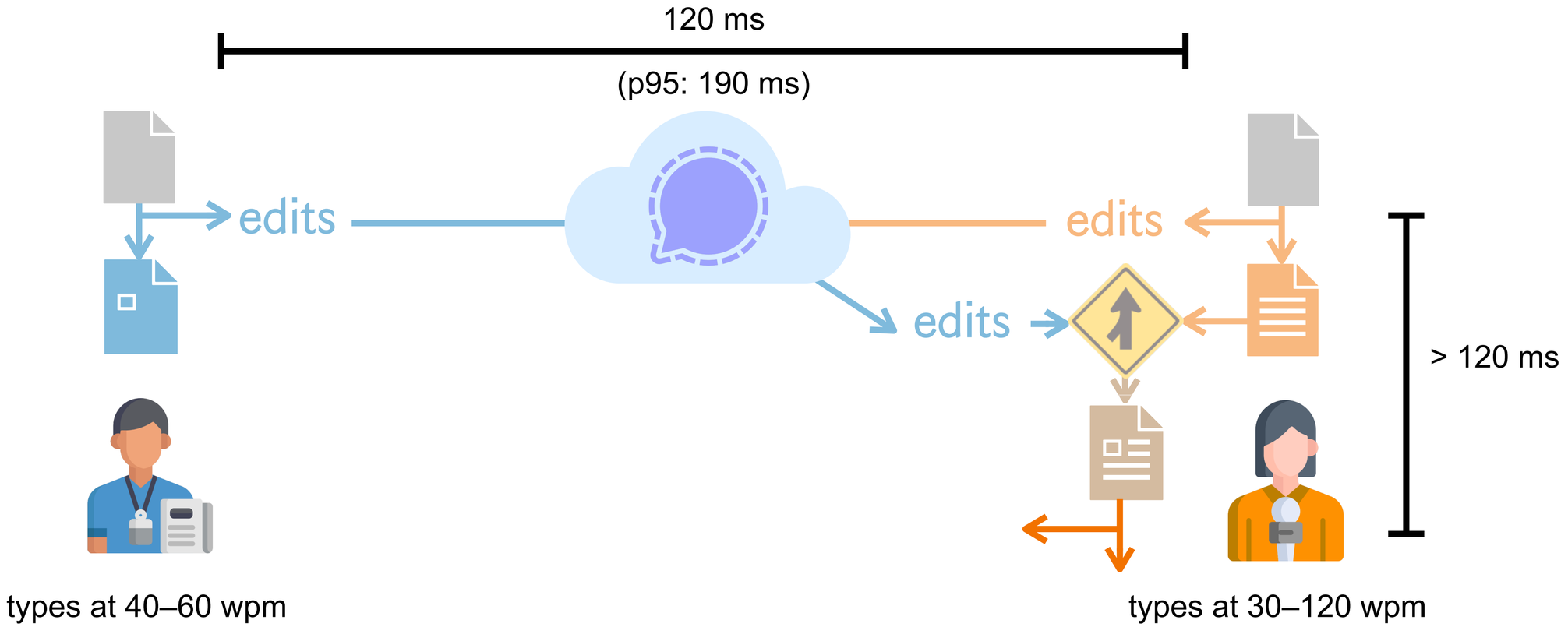
Synchronous editing



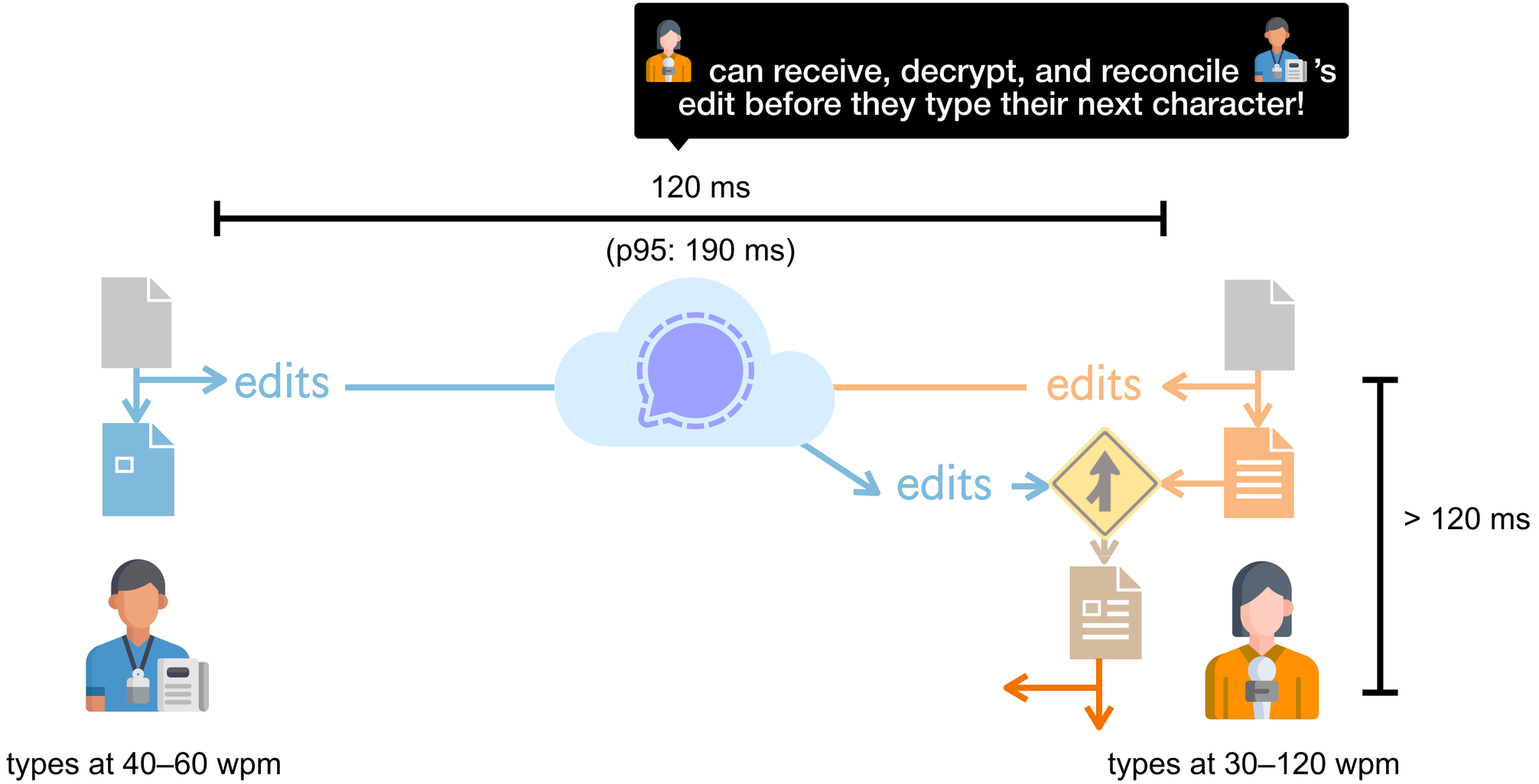
Synchronous editing



Synchronous editing



Synchronous editing



End-to-End Encrypted Collaborative Documents

Christian Knabenhans* EPFL
Zayd Maradni* MPI-SP
Carmela Troncoso EPFL, MPI-SP
*these authors contributed equally to this work

USENIX Security'26