

DatashareNetwork: A Decentralized Privacy-Preserving Search Engine for Investigative Journalists

Kasra EdalatNejad (EPFL)

Wouter Lueks (EPFL), Julien Martin, Soline Ledésert (ICIJ)

Anne Lhôte (ICIJ), Bruno Thomas (ICIJ), Laurent Girod (EPFL), Carmela Troncoso (EPFL)

EPFL



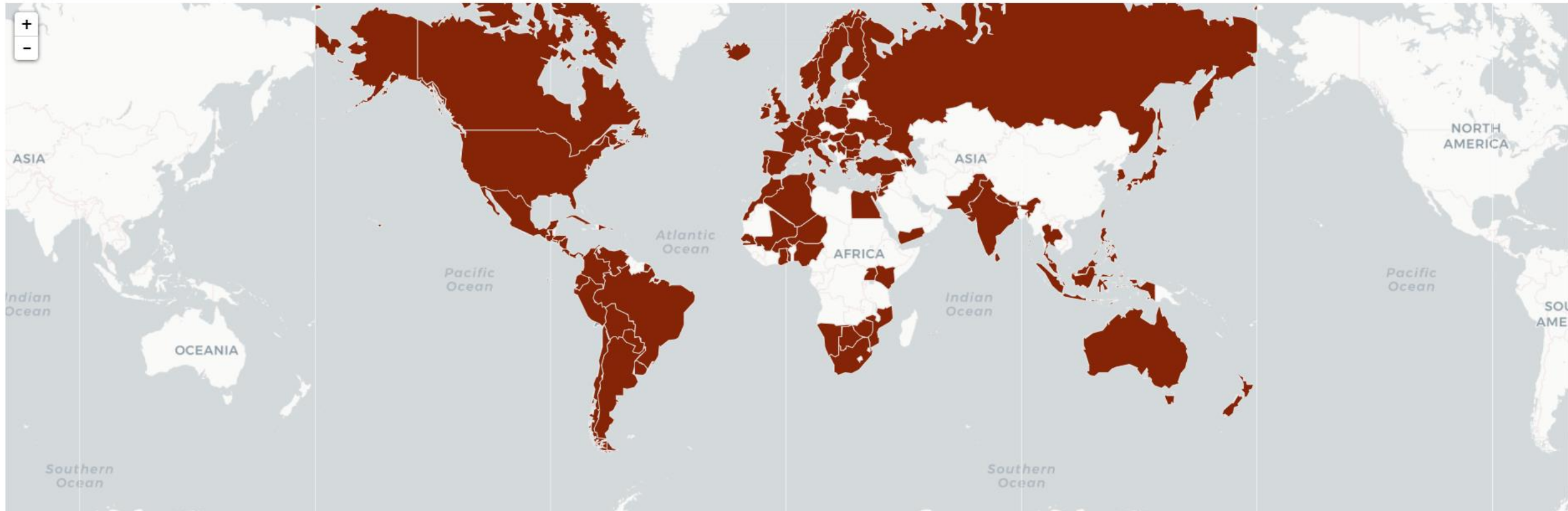


DONATE

FOLLOW

Journalists

The International Consortium of Investigative Journalists is a global network of 267 investigative journalists in 100 countries who collaborate on in-depth investigative stories.





An ICIJ Investigation

The Panama Papers: Exposing the Rogue Offshore Finance Industry

A giant leak of more than 11.5 million financial and legal records exposes a system that enables crime, corruption and wrongdoing, hidden by secretive offshore companies.



11.5 Million documents
(Centralized)



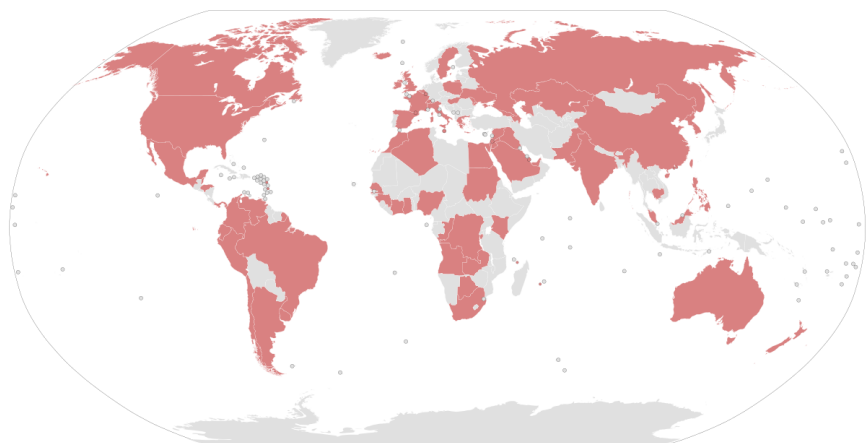
An ICIJ Investigation

The Panama Papers: Exposing the Rogue Offshore Finance Industry

A giant leak of more than 11.5 million financial and legal records exposes a system that enables crime, corruption and wrongdoing, hidden by secretive offshore companies.



11.5 Million documents
(Centralized)



Journalists from over
80 countries

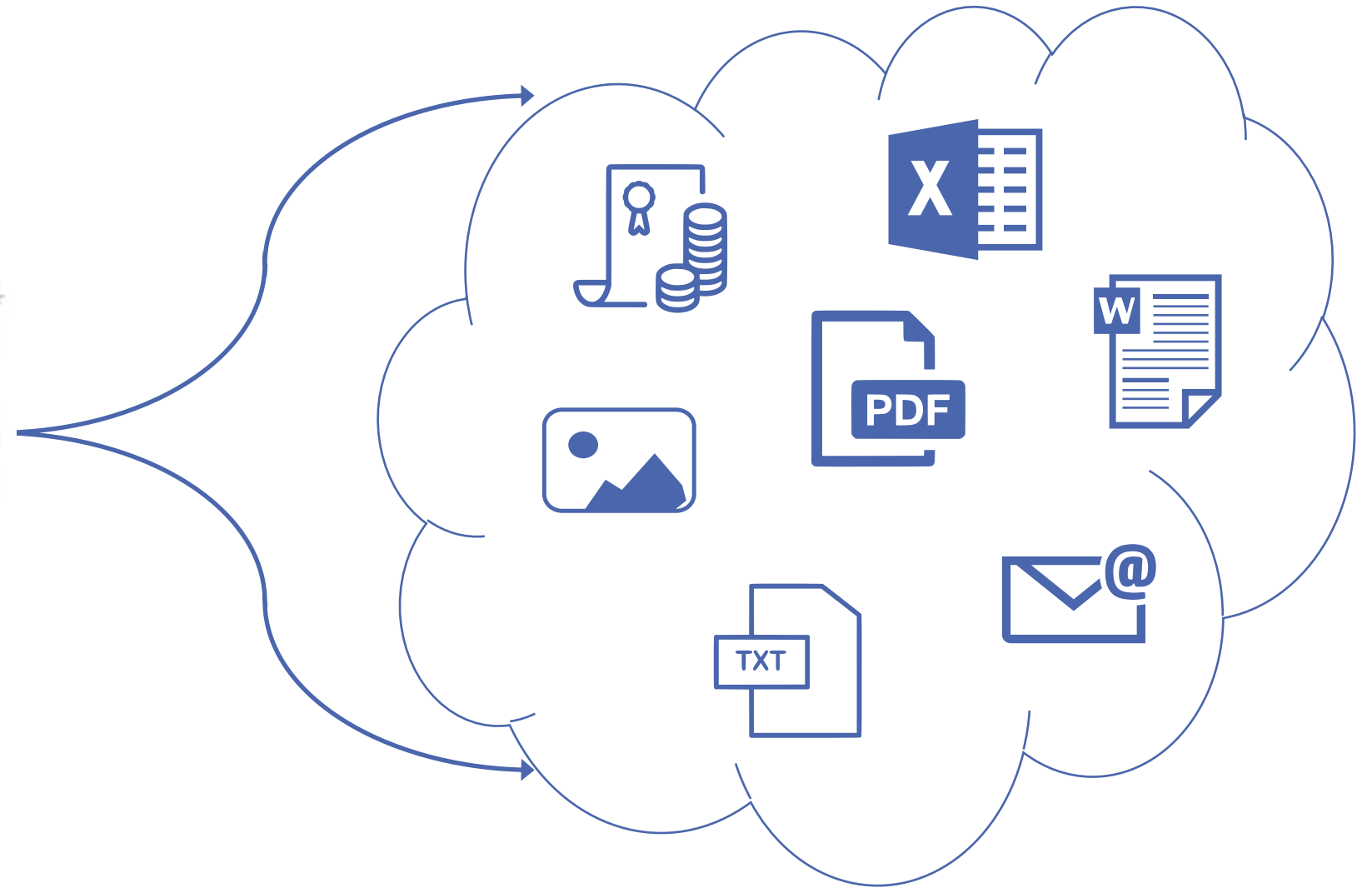


An ICIJ Investigation

The Panama Papers: Exposing the Rogue Offshore Finance Industry

A giant leak of more than 11.5 million financial and legal records exposes a system that enables crime, corruption and wrongdoing, hidden by secretive offshore companies.

Digitalization



The logo icon consists of a red square on the left, a blue square on the right, and a white curved shape in the center that overlaps both, resembling a stylized 'D' or a data visualization element.

Datashare beta

Better analyze information, in all its forms

H4201030M.pdf

- EXTRACTED TEXT
- PREVIEW
- TAGS & DETAILS
- NAMED ENTITIES**

People (36)

- KOHL HUTCHISON LUXCO HUTCHISON KOHL PEETERS LUXCO LUXCO LUXCO LUXCO LUXCO WIM PIOT WIM PIOT
- MARIUS KOHL LUXEMBOURG HUTCHISON CONFIDENTIAL HUTCHISON ROBERT ECBRT ECKERT LUXELLBOURG ILCJB DINE AUMIAN SCHILLING
- ROBIO SNG DIRECTOR HUTCHISON HUTCHISON ROBERT ECKERT ECKERT HUTCHISON ROBINDIRECTOR HUTCHISON HUTCHISON ROBERT
- HUTCHISON HUTOHLSA DILLION ROBIN ROBERT ECKERT ECKERT HUTCHISON

Extracted using **CORENLP** in **ENGLISH**

...tria, the fiscal value of LuxCo's

participation in **H3G Holdings** should consist of its acquisition price, increased by the

amounts granted by LuxCo to H3G Austria. The total amount of these contributions will

Organizations (52)

- MR PEETERS ADMINISTRATION DES CONTR
- LUXEMBOURG TELEPHONE HUTCHISON
- HUTCHISON WHAMPOA LIMITED AUSTR
- R.C. LUXEMBOURG BUREAU D'IMPOSITIO
- RMS/VLN/H4201030M-WPIHUTCHISON WH
- HUTCHISON WHAMPOA LIMITED HUTCH
- H3G HOLDINGS R.C. LUXEMBOURG B LUXCO LUXCO H3G HOLDINGS H3G HOLDINGS LUXCO H3G HOLDINGS LUXCO LUXCO LUXCO
- H3G HOLDINGS H3G HOLDINGS LUXCO H3G HOLDINGS HUTCHISON 3G AUSTRIA INVESTMENTS S.A.R.L HUTCHISON 3G AUSTRIAGMBH
- AUSTRIA INVESTMENTS S.A.R.L. HDTCHISON 3G AUSTRIA GMBH HUTCHISON AUSTRIA INVESTMENTS YHUTCHISON 3G AUSTRIA INVESTMENTS
- HUTCHISON 3G AUSTRIA GMBH HUTCHISON 3G AUSTRIA HOLDINGS HUTCHISON 3G AUSTRIA GMBH HUTCHISON 3G AUSTRIA GMBH FCBRUAR
- AUSTRIA GMBH AUSLRIA INVESTMENTS S.A.R.L. HUTCHISON 3G AUSTRALIA HOLDINGSGMBH HUTCHISON 3G AUSTRIA GMBH

Locations (61)

- EUROPE AUSTRIA AUSTRIA AUSTRIA LUXEMBOURG EUROPE AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA
- AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA ILL AUSTRIA LUXEMBOURG AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA
- LUXEMBOURG AUSTRIA AUSTRIA LUXEMBOURG AUSTRIA AUSTRIA AUSTRIA AUSTRIA AUSTRIA LUXEMBOURG LUXEMBOURG
- AUSTRIA AUSTRIA EUROPE AUSTRIA VIENNA AUSTRIA HATCBISOO AUSTRIA AUSTRIA EUROPE JC LUXEMBOURG VIENNA

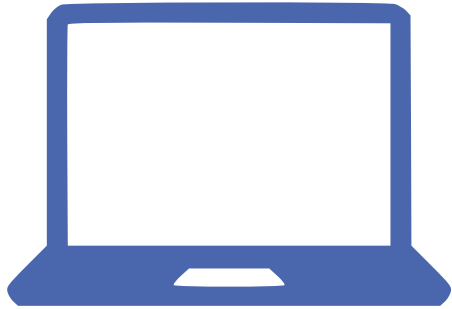
Show more locations

Datashare



Central

Datashare

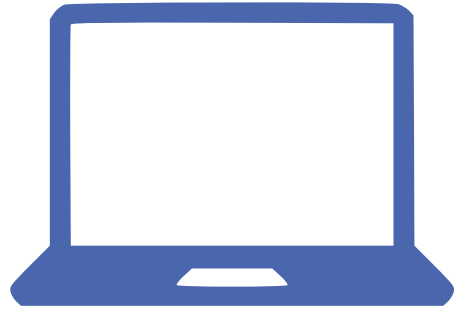


Local

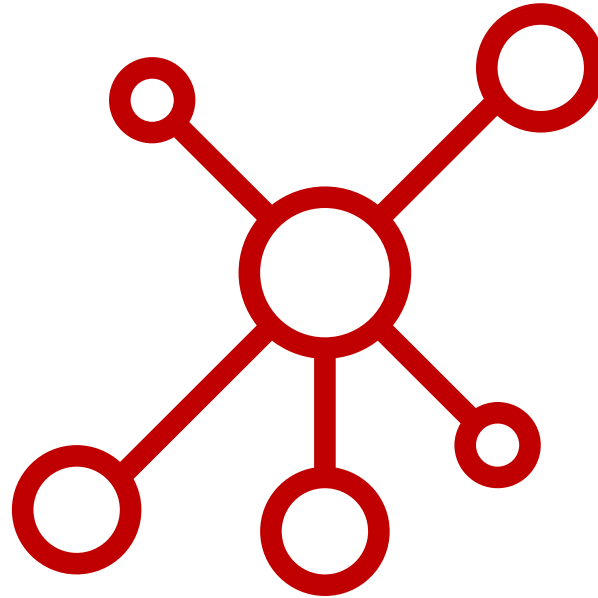


Central

DatashareNetwork



Local



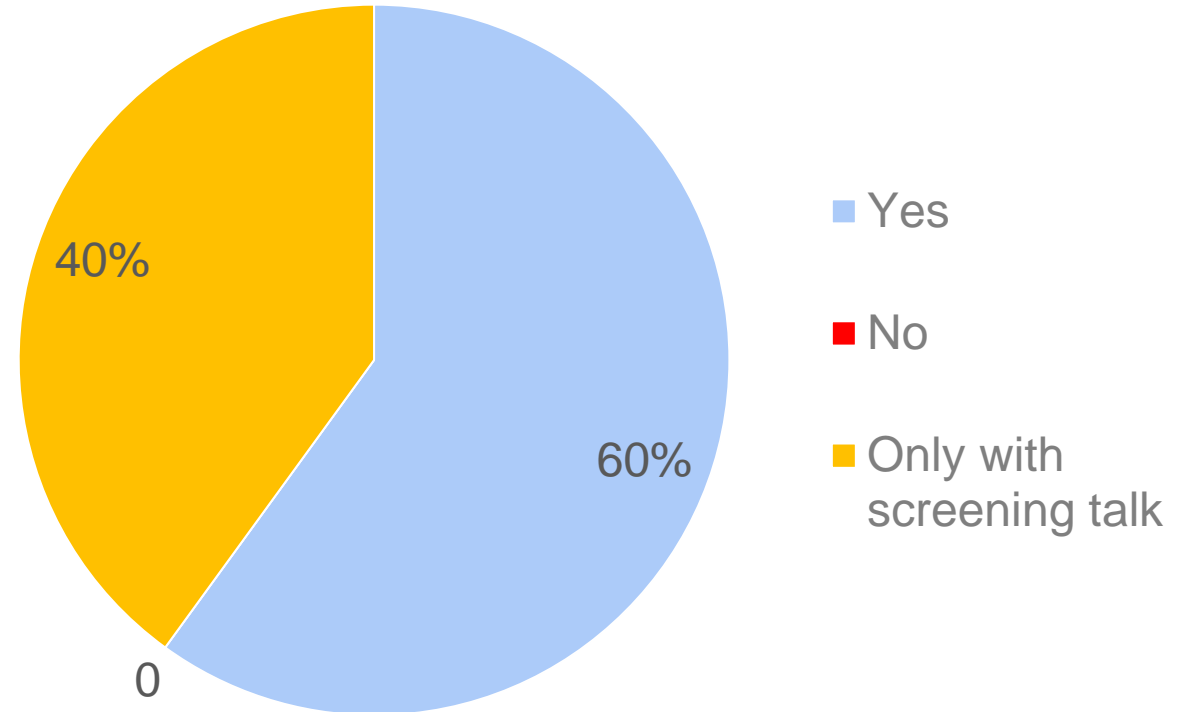
Journalist ↔ Journalist



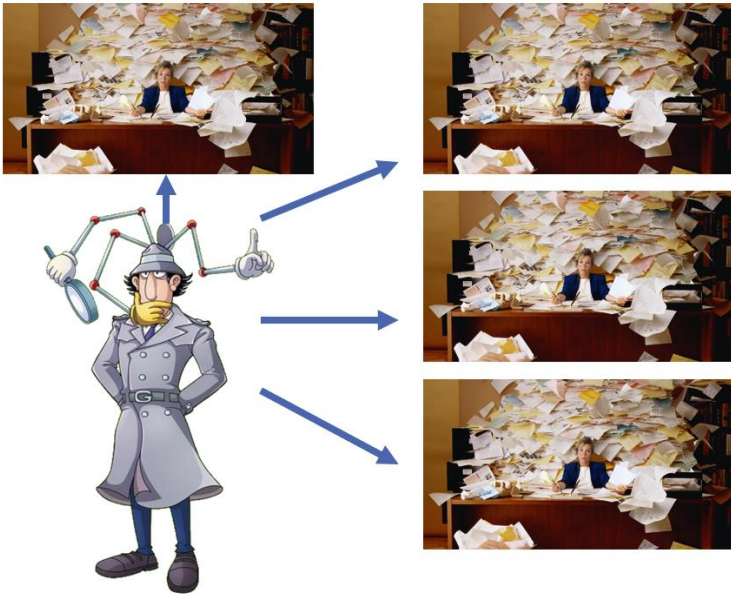
Central

Survey: sharing

Are you willing to share your documents?

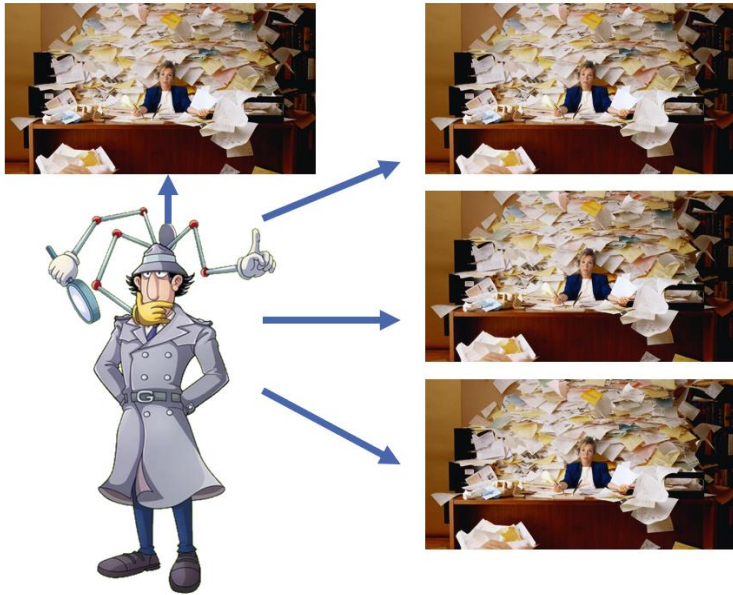


1. Privacy-preserving search



Search

1. Privacy-preserving search



Search



Find



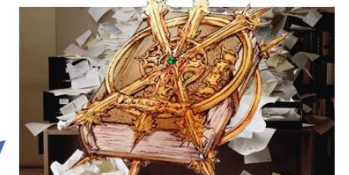
2. Screening talk



Search



Find



Contact

Out of band collaboration/sharing



Find

Contact

No retrieval

Survey: threat model



Journalists



ICIJ



Third party

Survey: threat model



Journalists



ICIJ



Third party



Survey: threat model



Journalists



ICIJ



Third party

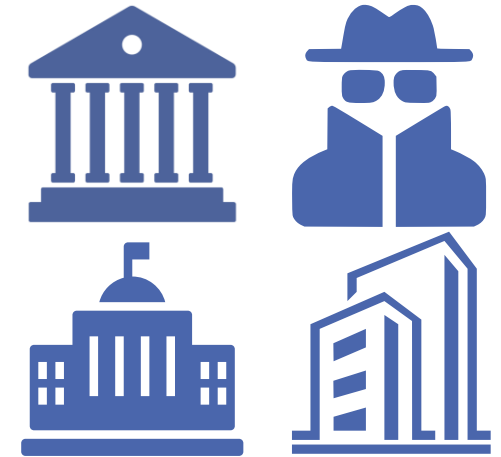
Survey: threat model



Journalists



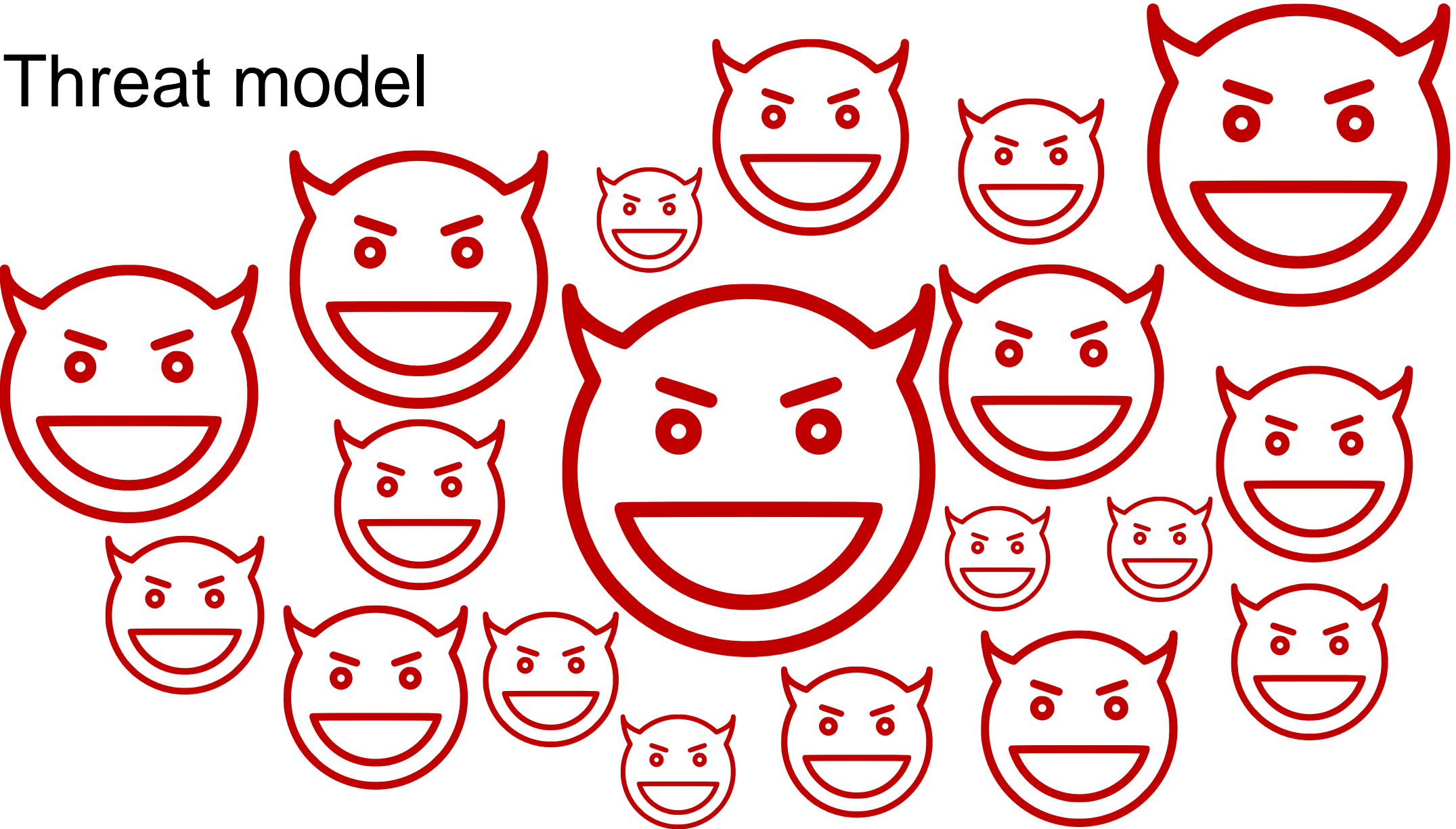
ICIJ



Third party



Threat model



Coerce or compromise



Hacking

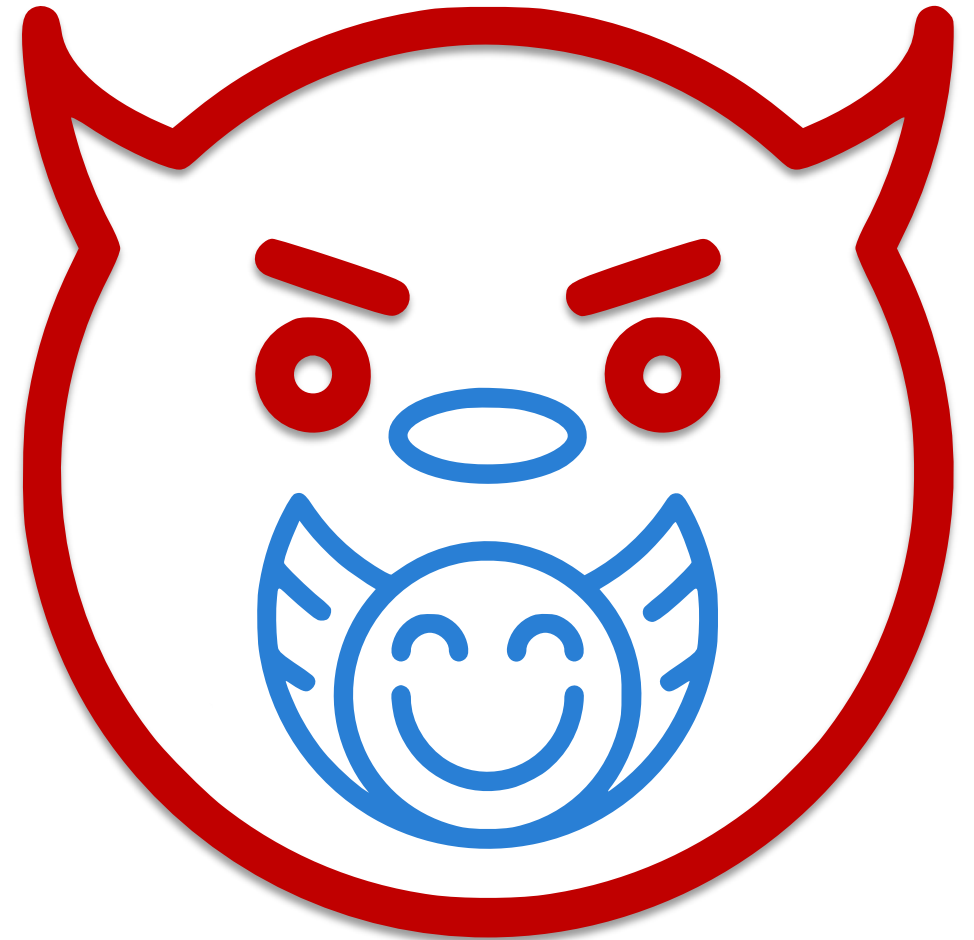


Violence

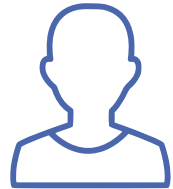


Subpoena

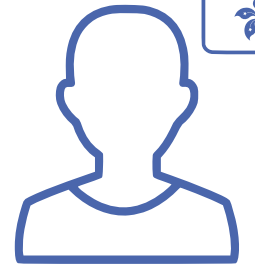
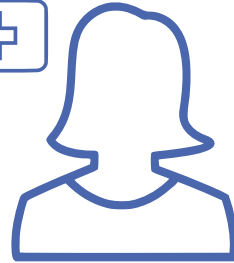
Malicious for protection



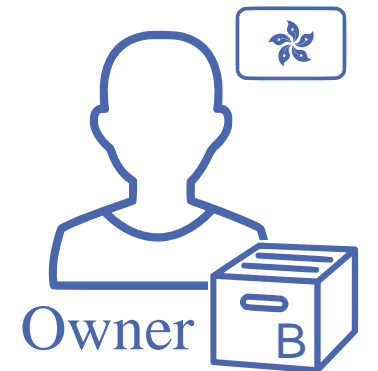
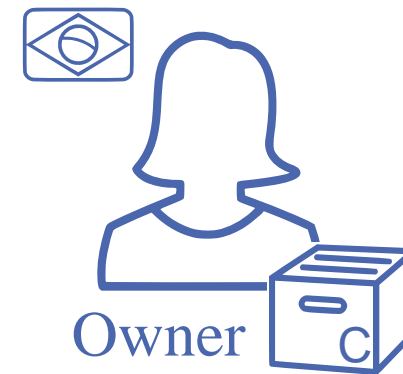
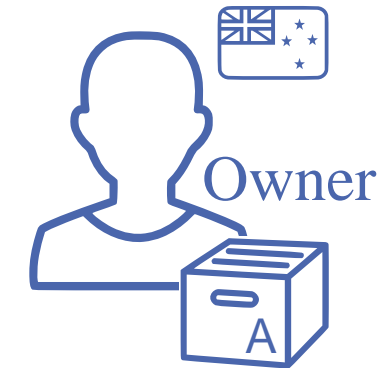
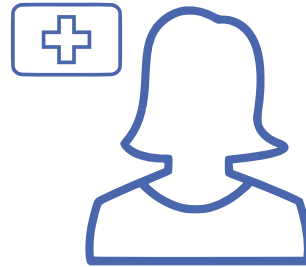
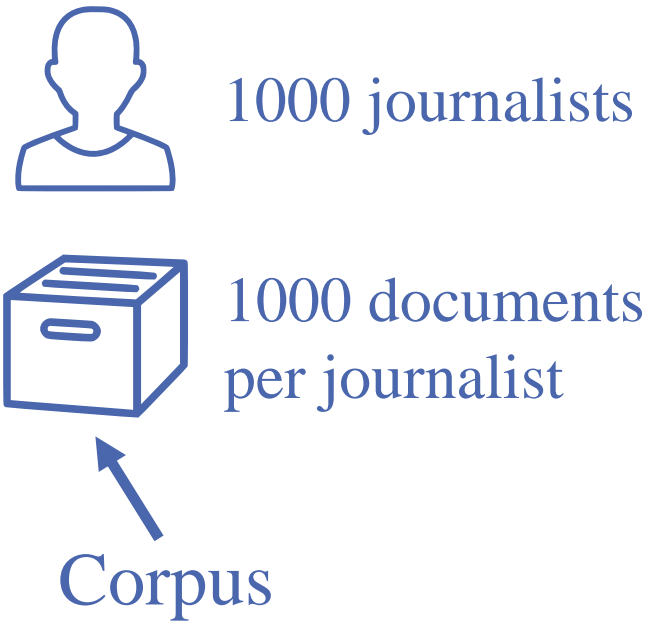
Setting



~~267~~ 1000 journalists

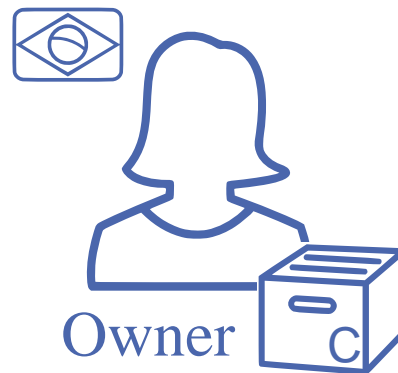
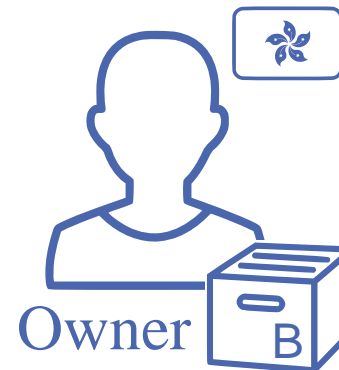
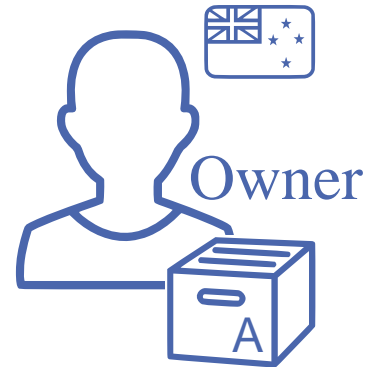
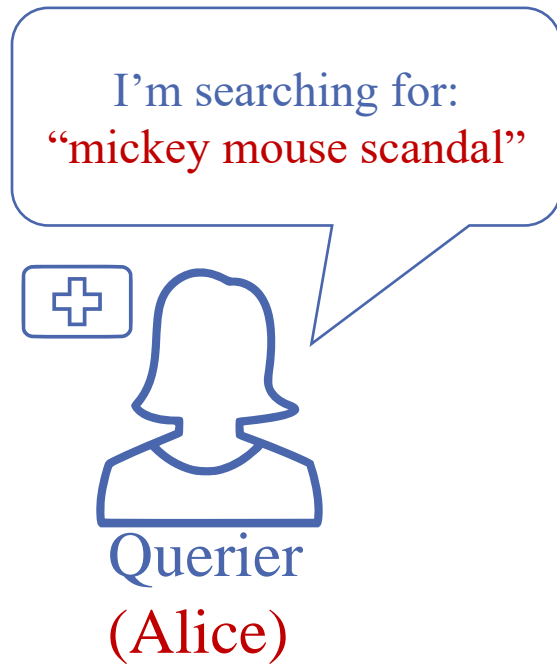


Setting



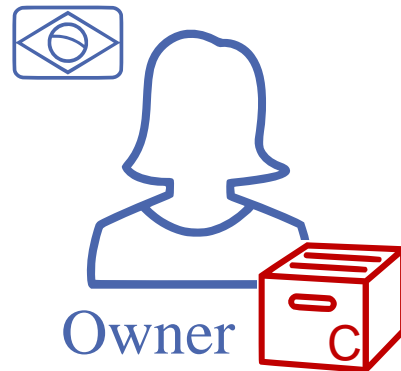
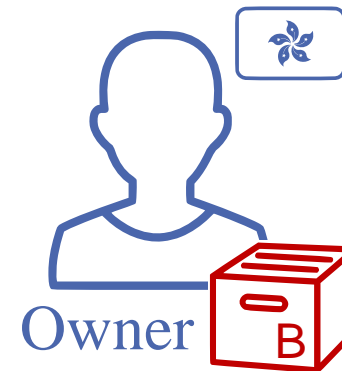
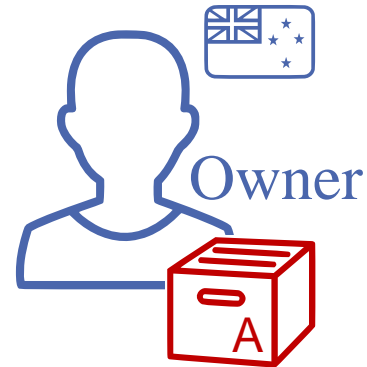
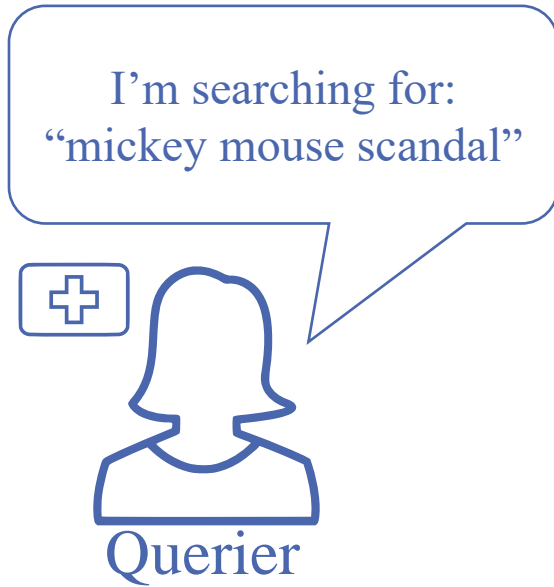
Privacy

Privacy: querier



- Protect:
- The query
 - The querier's identity

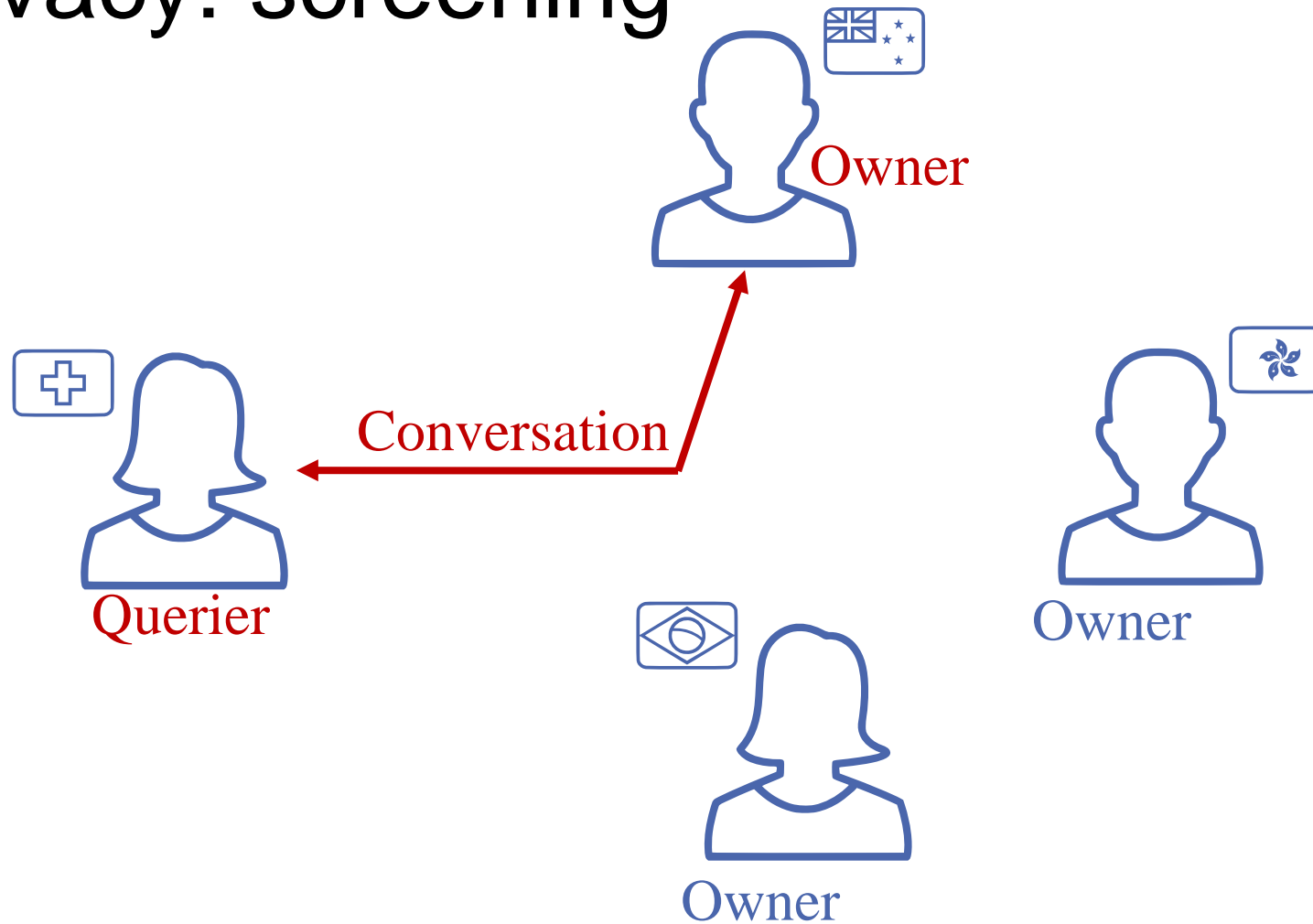
Privacy: owner



Protect:

- The corpus

Privacy: screening

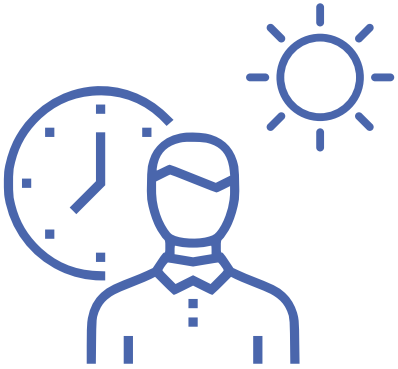


- Protect:
- The content of conversation
 - The existence of conversation

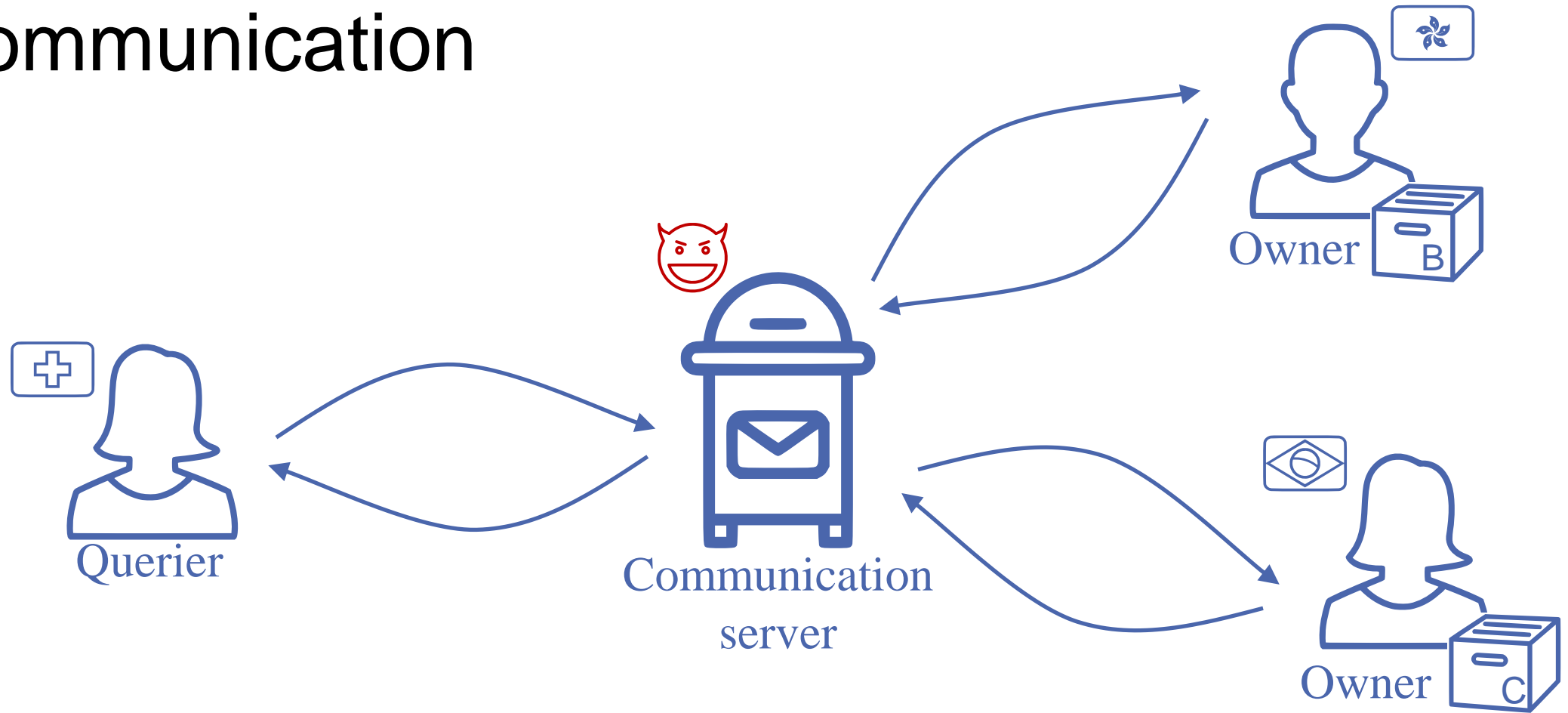
Build a system



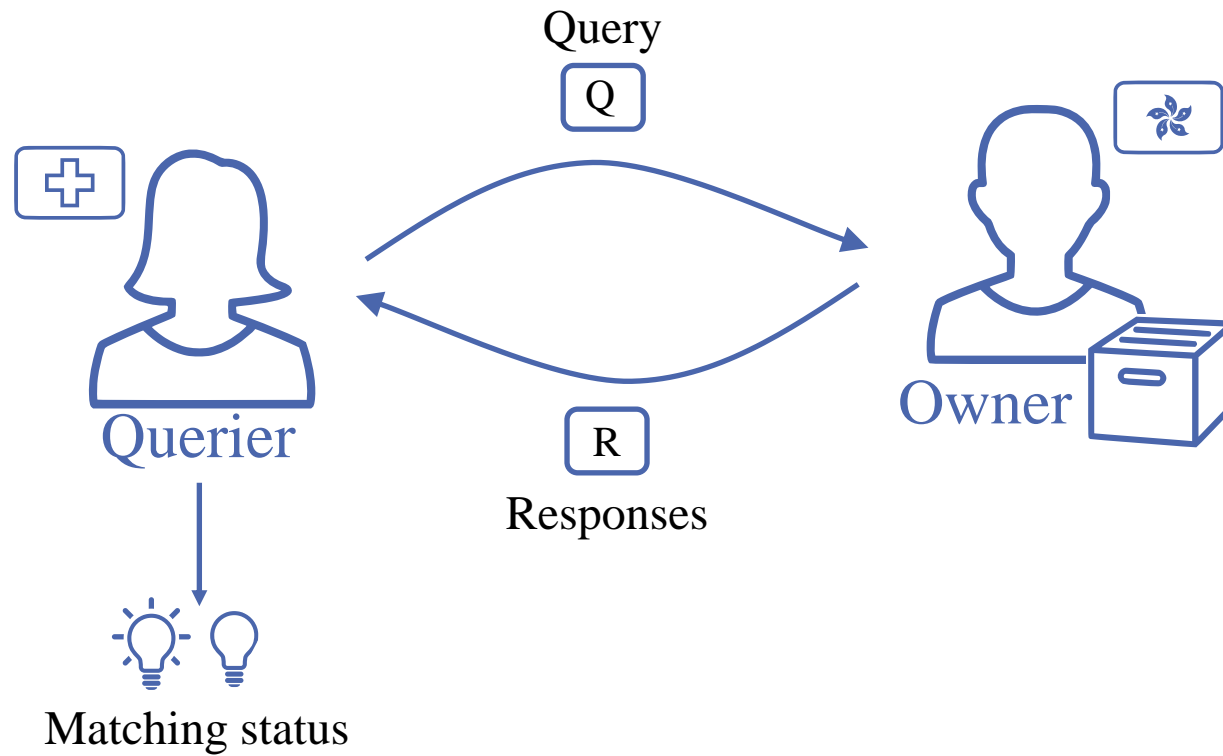
Challenge: asynchrony



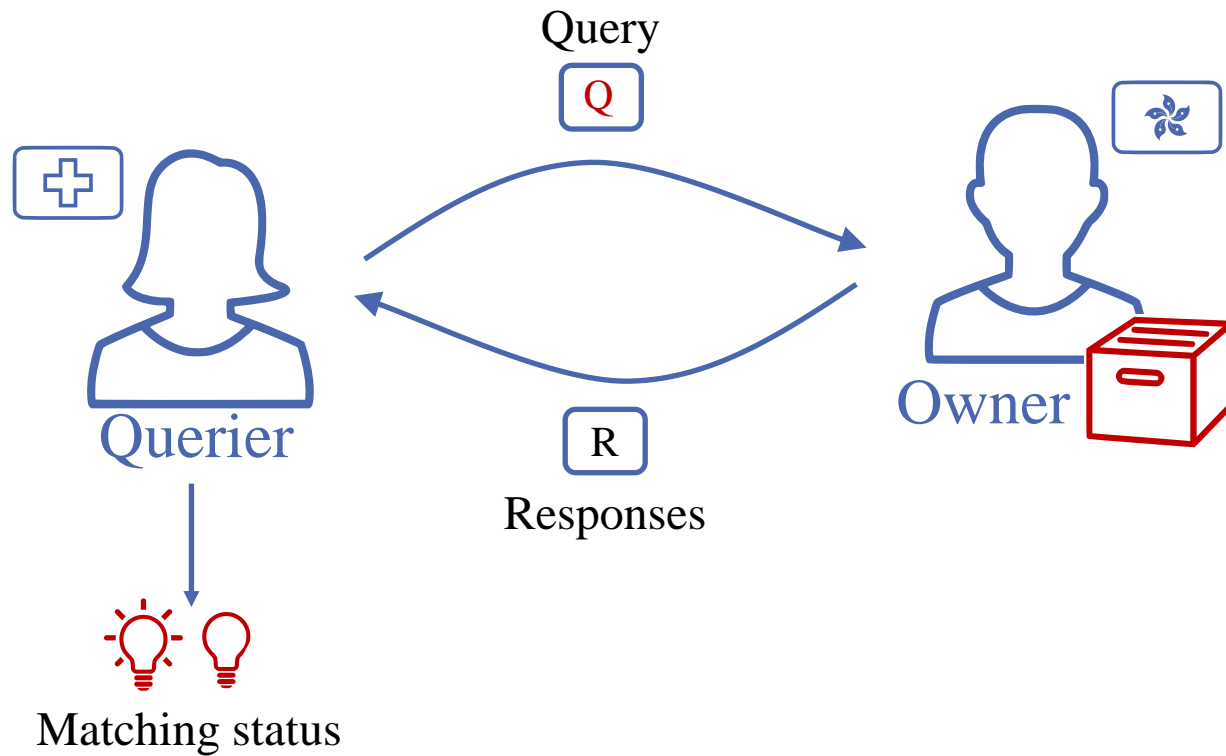
Communication



Challenge: find a match



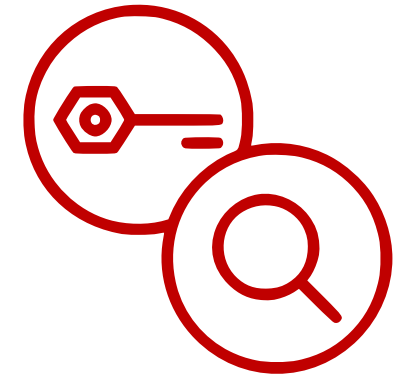
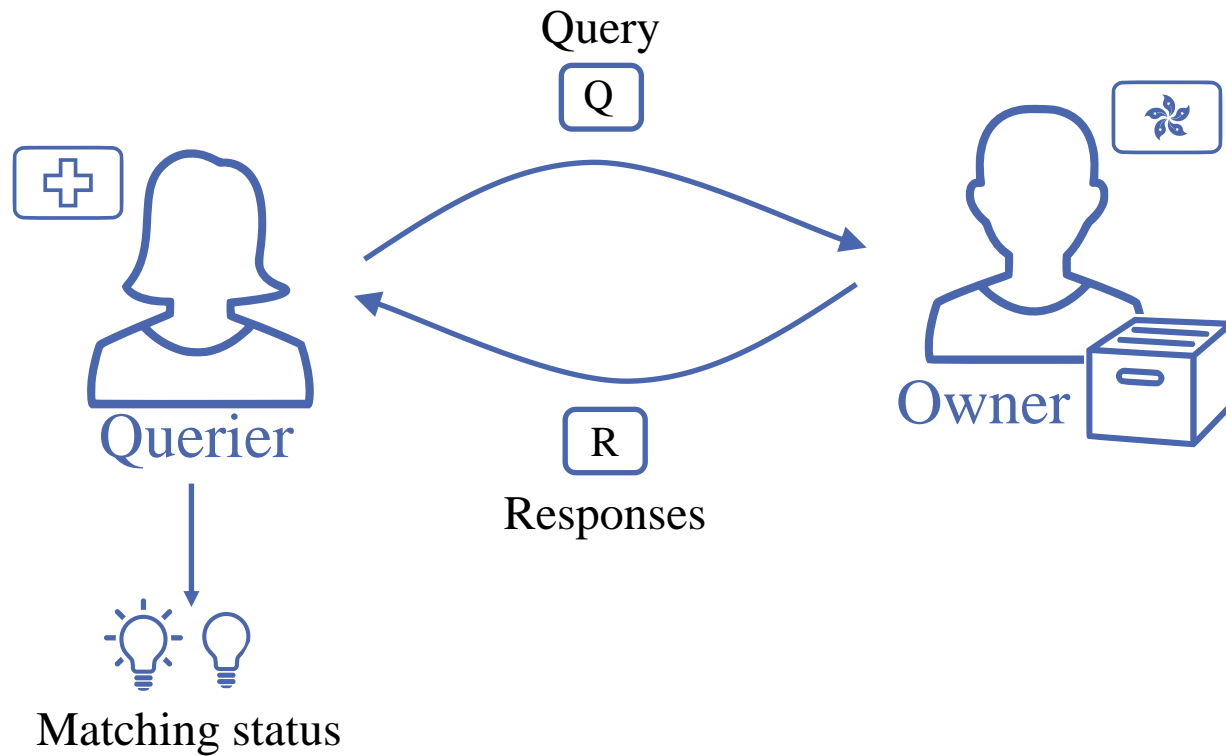
Document search



Protect:

- The query
- The corpus
- The result

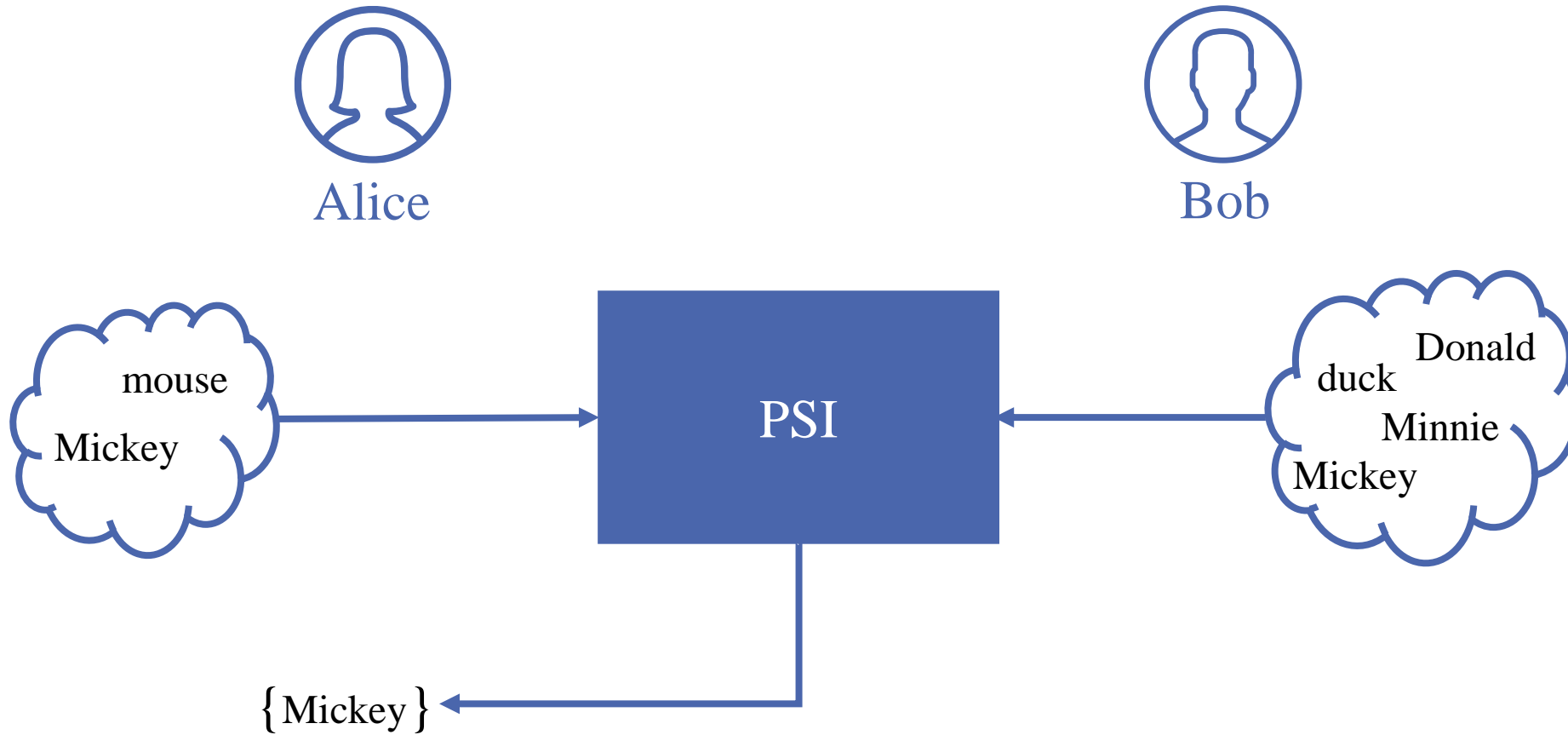
Document search



Multiset private
set intersection

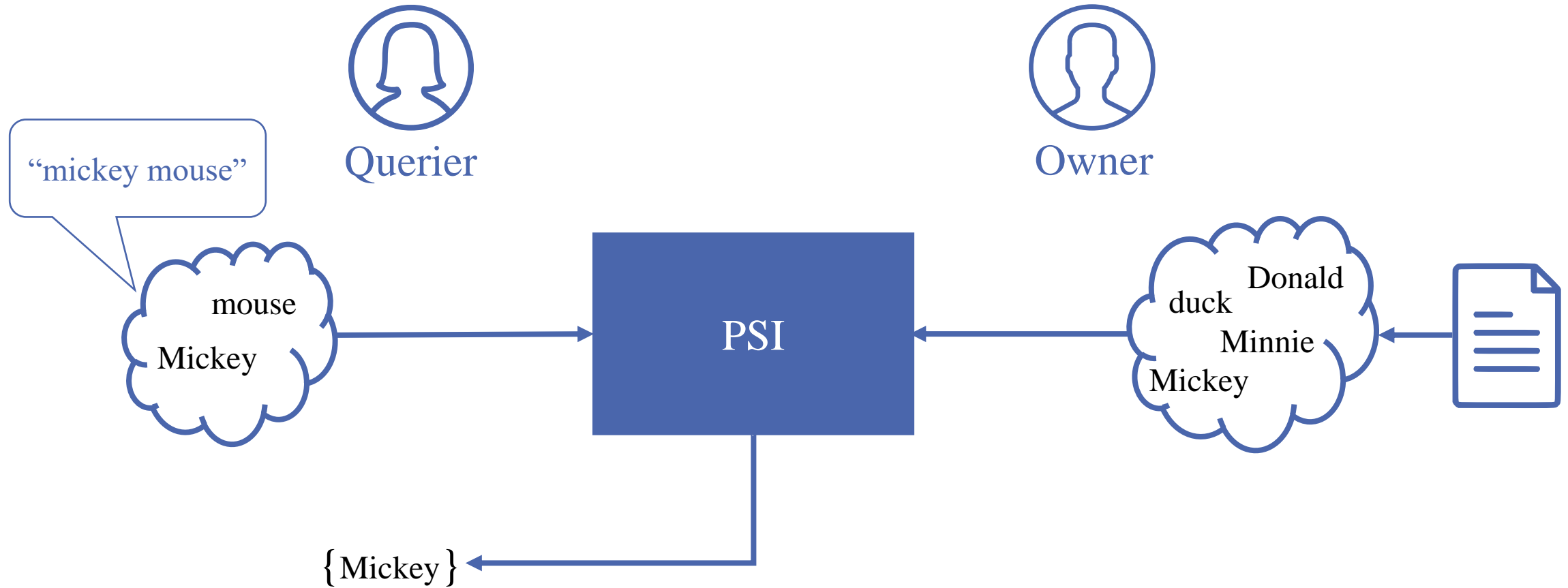
Existing

Private Set Intersection (PSI)



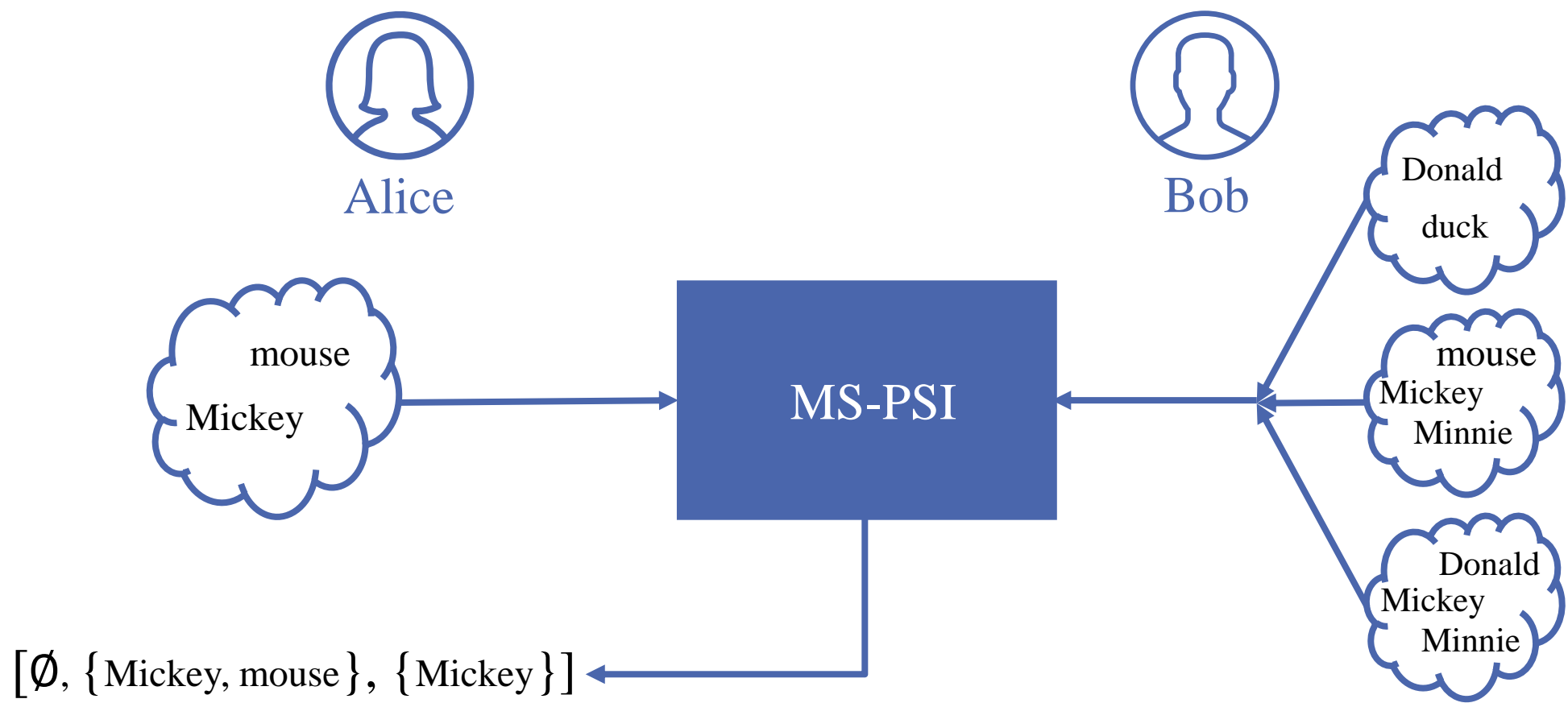
Existing

Private Set Intersection (PSI)



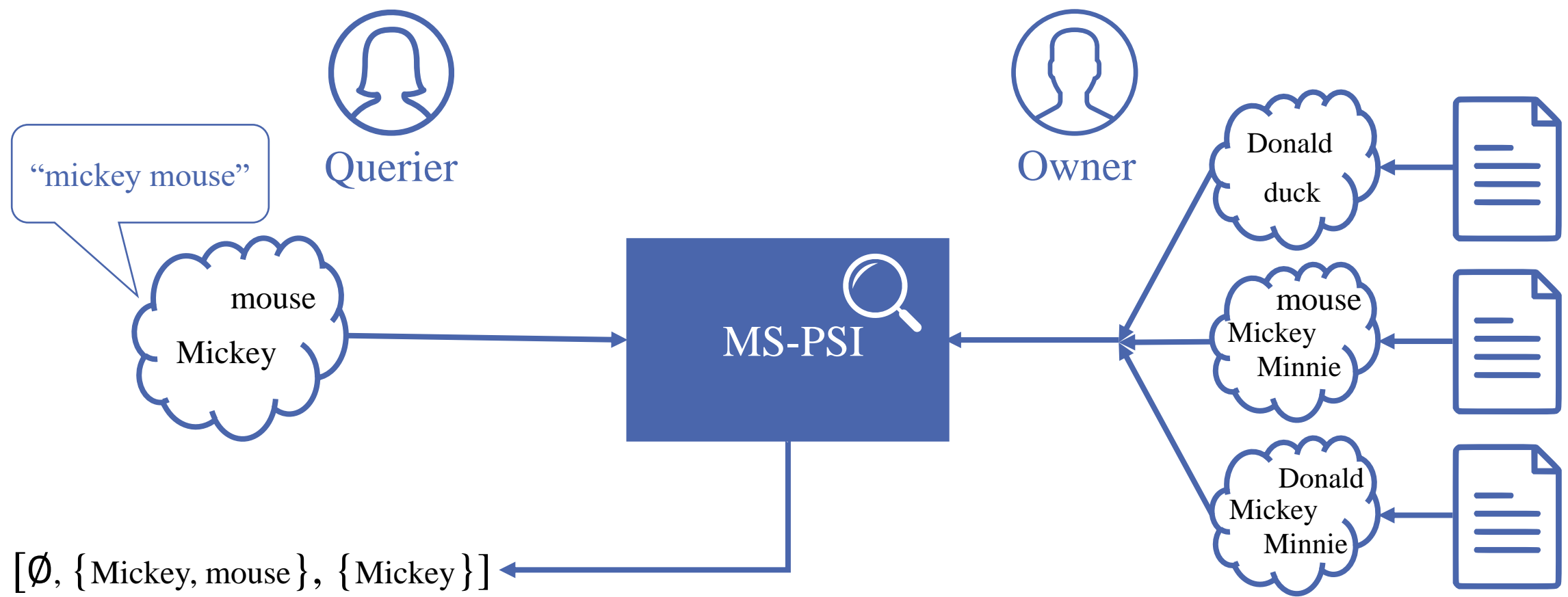
New

Multiset Private Set Intersection (MS-PSI)

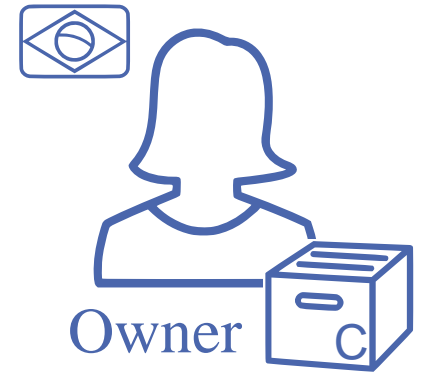
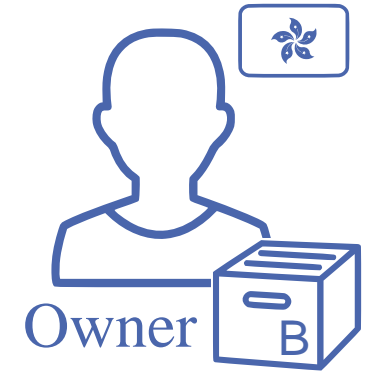


New

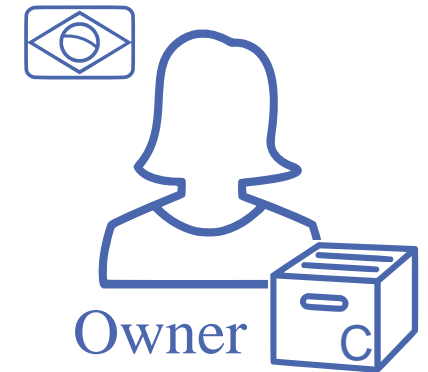
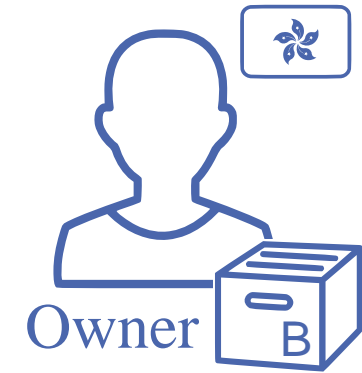
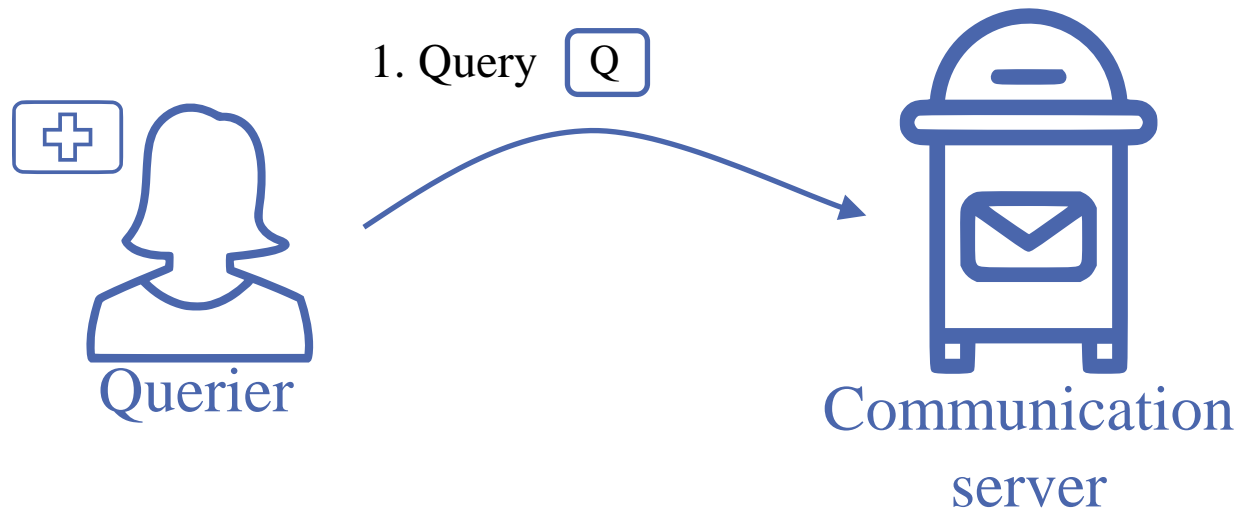
Multiset Private Set Intersection (MS-PSI)



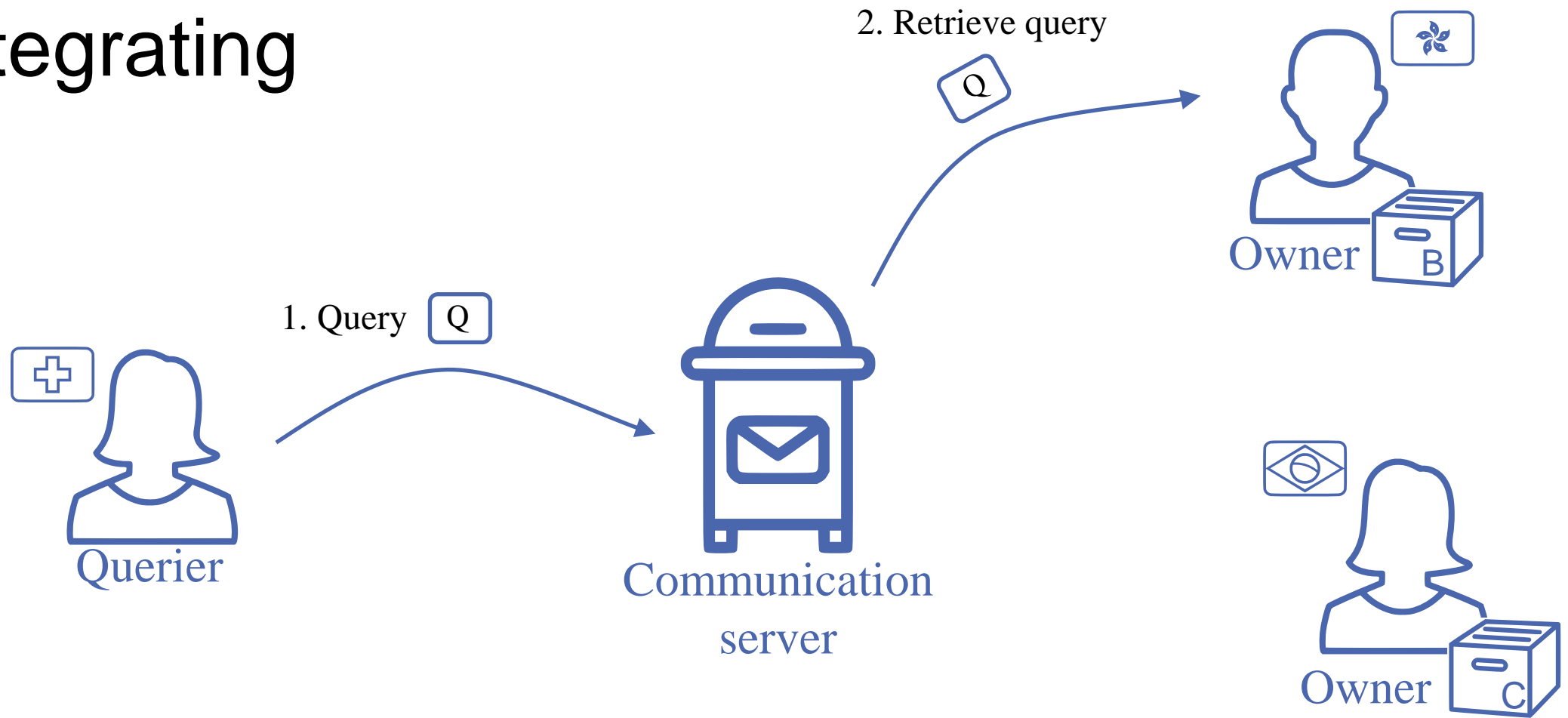
Integrating



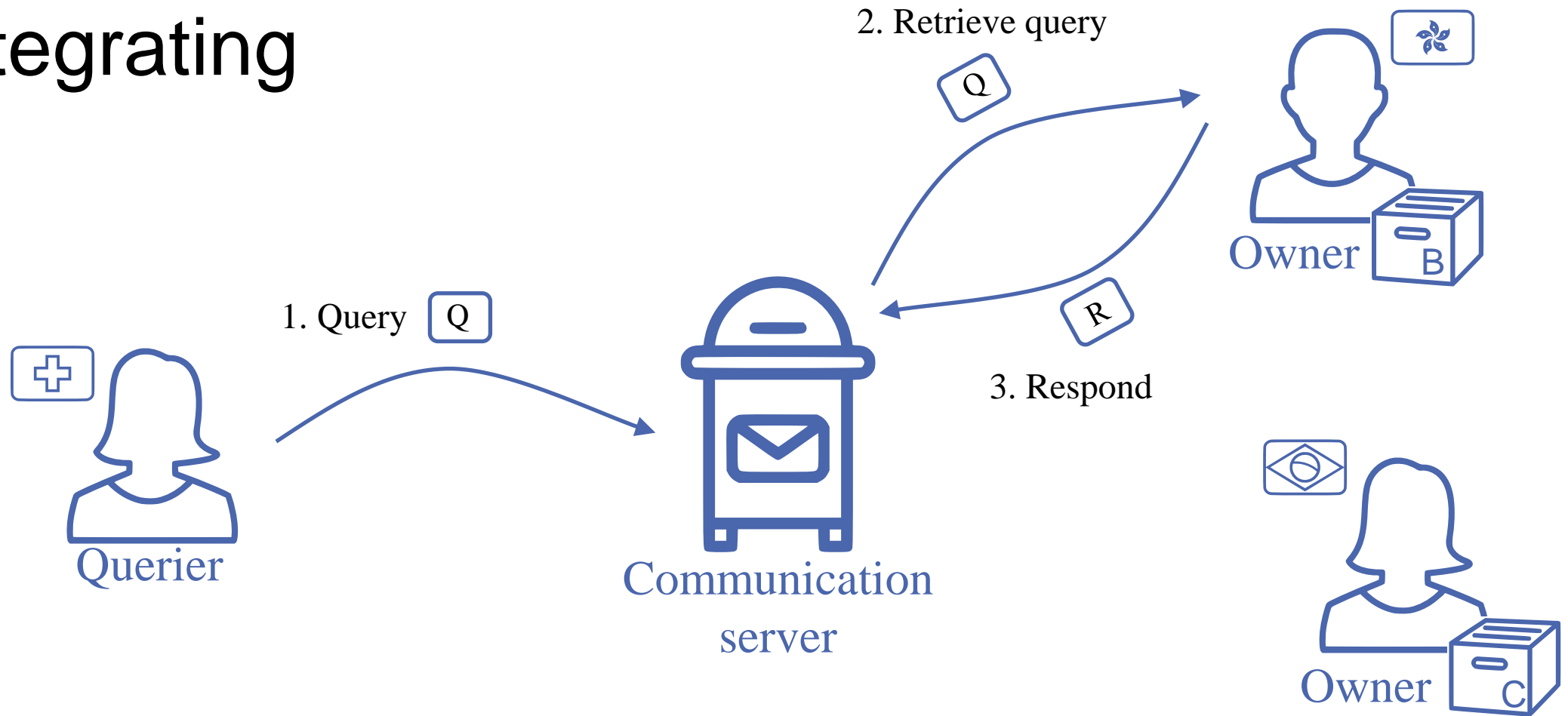
Integrating



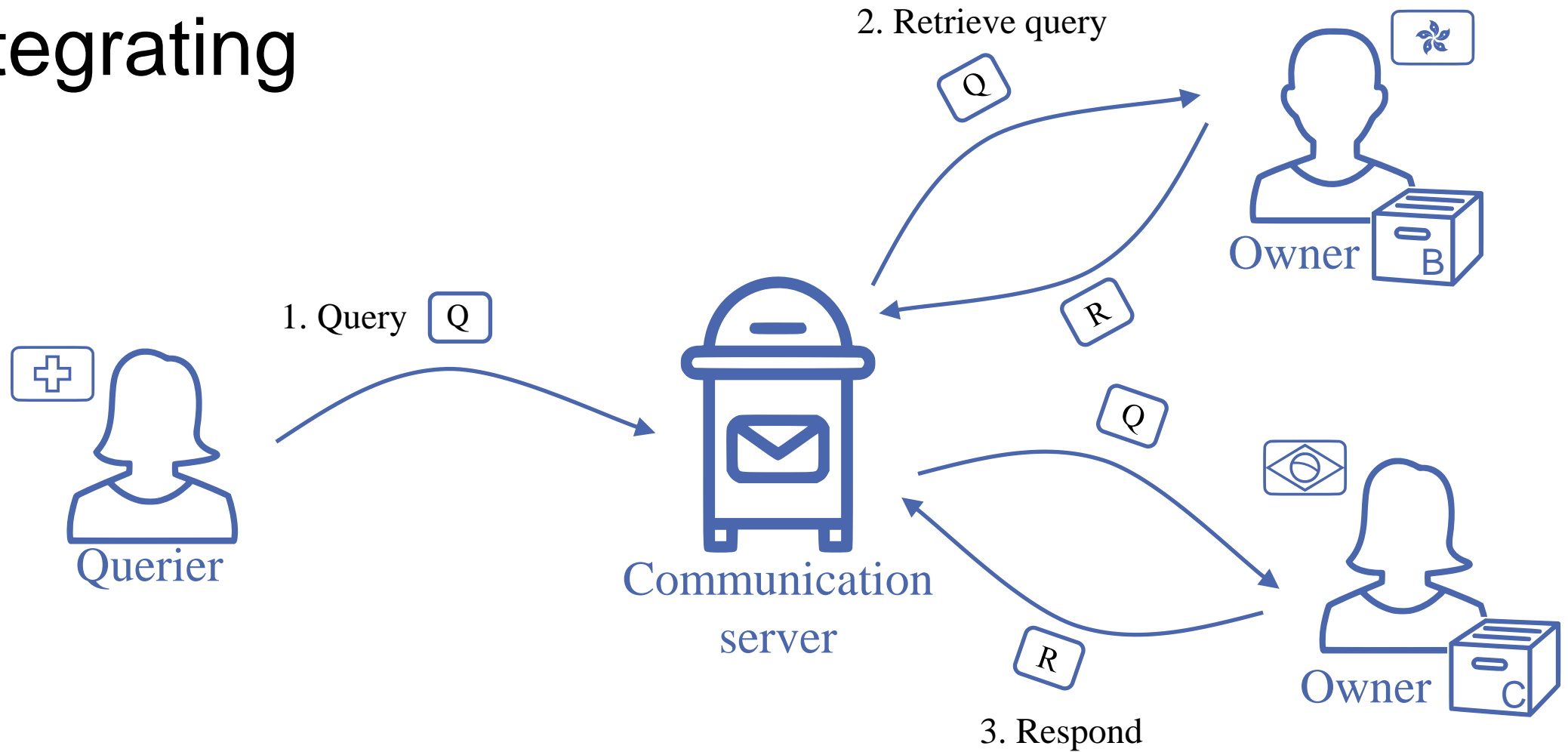
Integrating



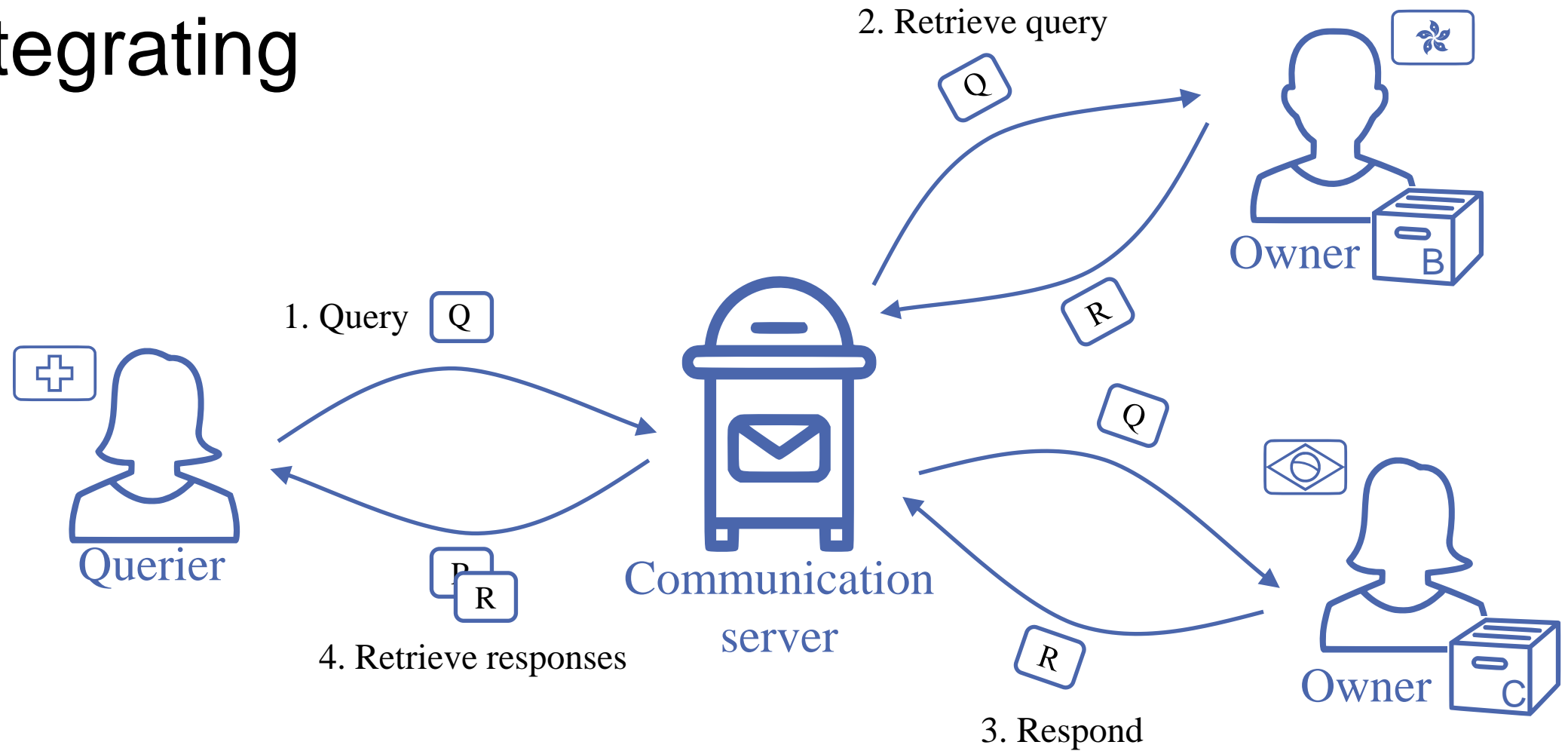
Integrating



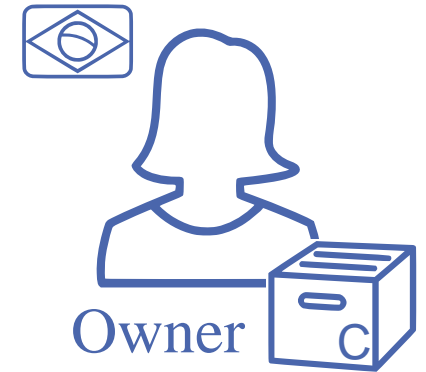
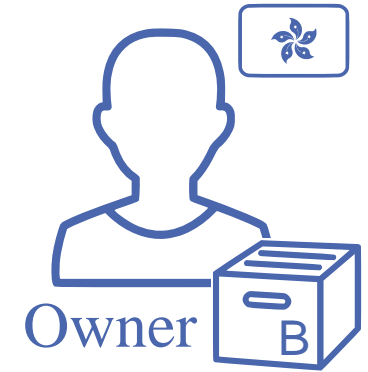
Integrating



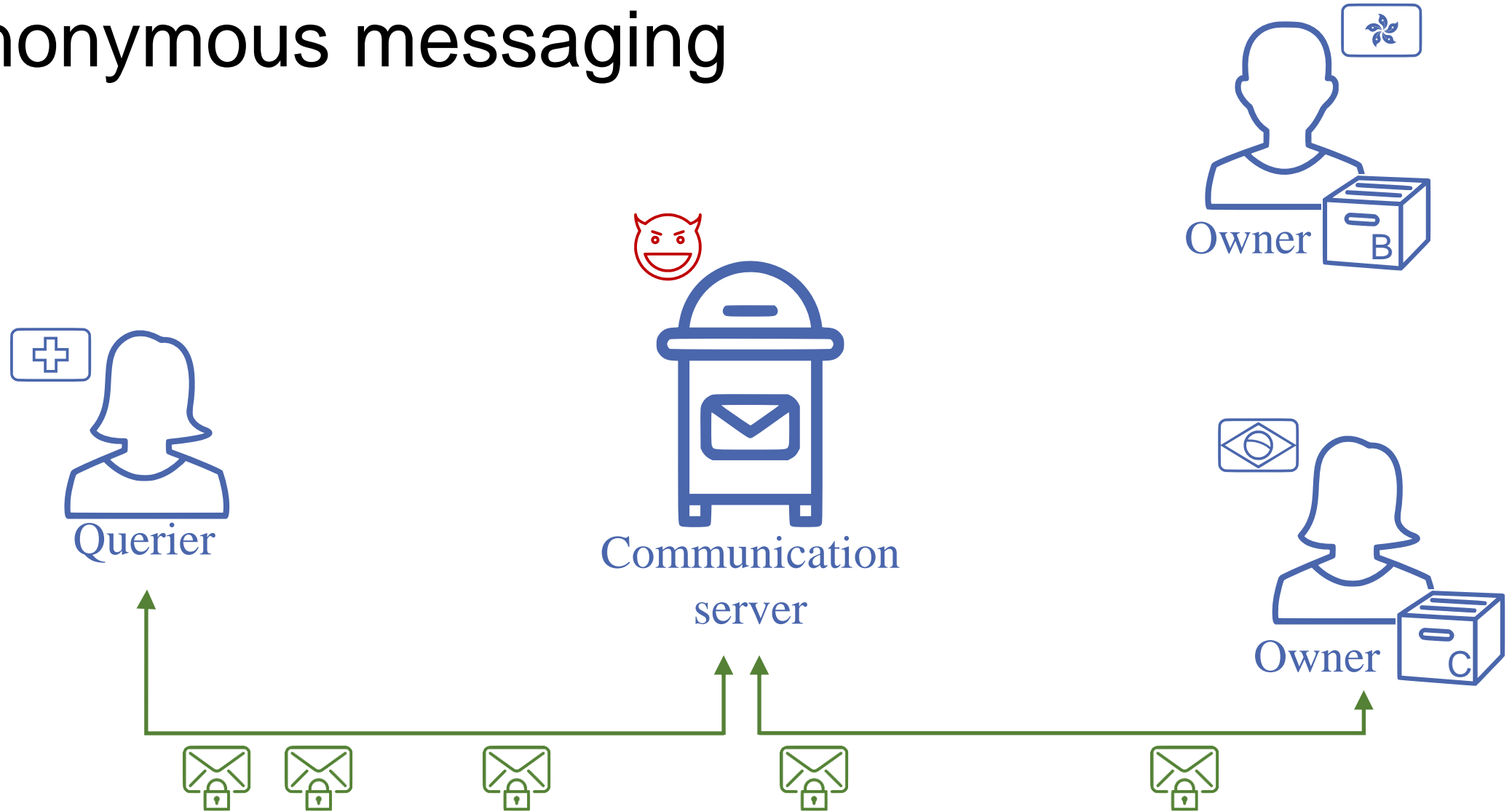
Integrating



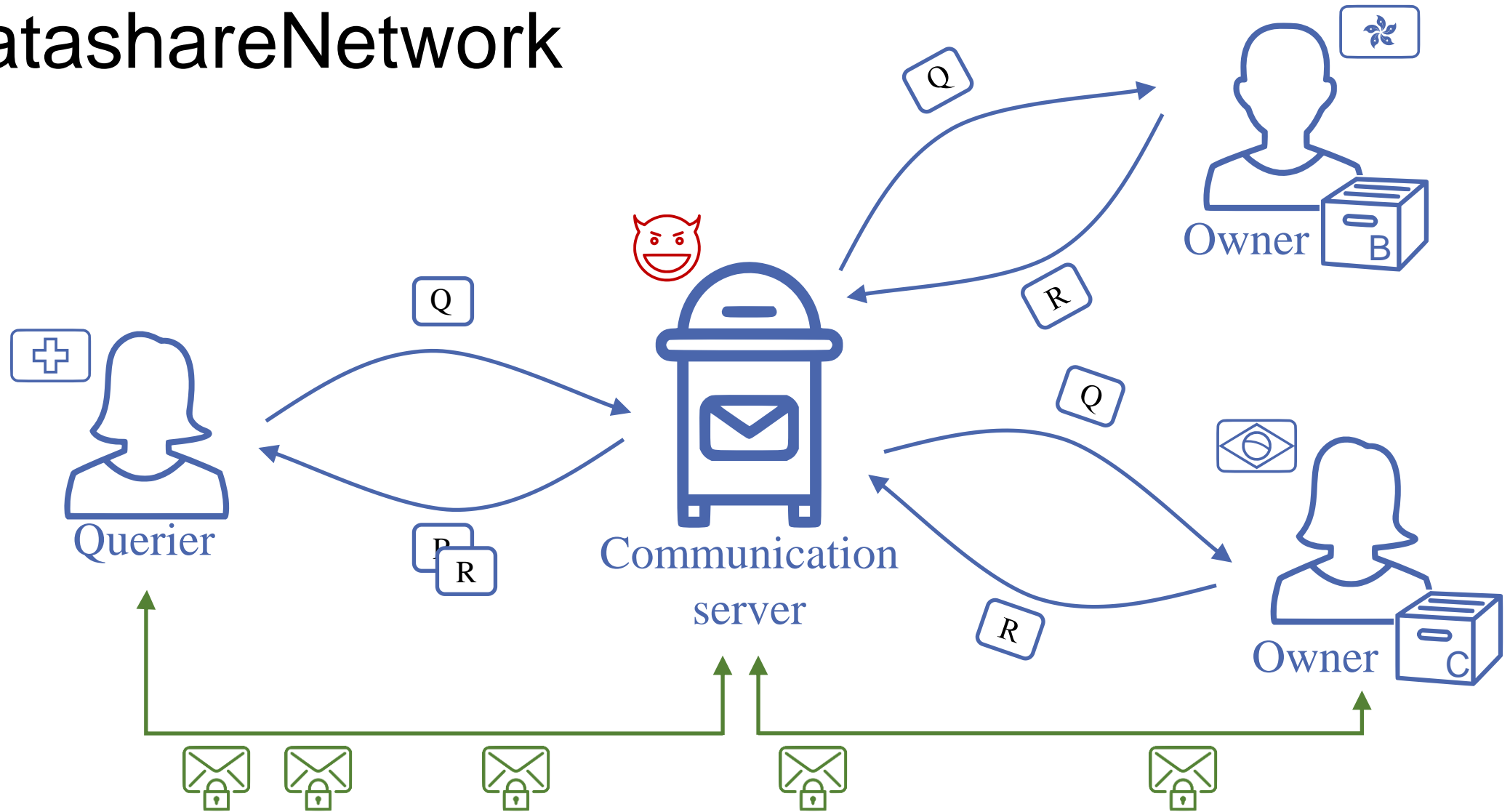
Challenge: enable screening talk



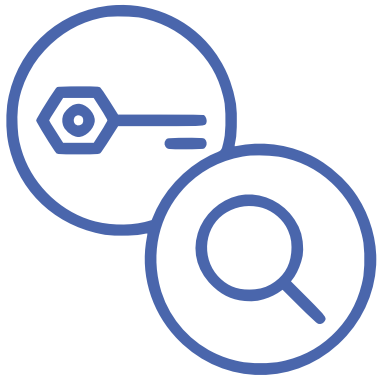
Anonymous messaging



DatashareNetwork



Privacy: layers



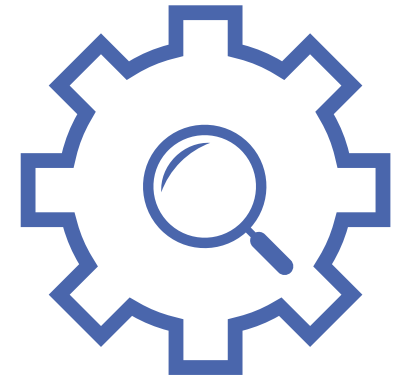
MS-PSI



Document search

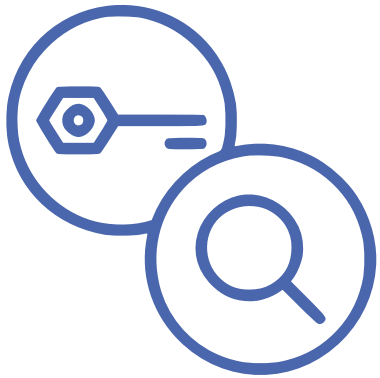


Messaging



DatashareNetwork

Privacy: layers



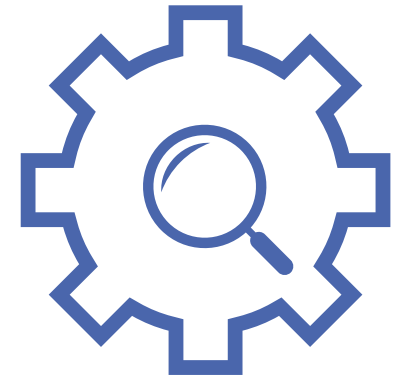
MS-PSI



Document search



Messaging



DatashareNetwork

Same privacy as
PSI*

Privacy: layers



MS-PSI

Same privacy as
PSI*

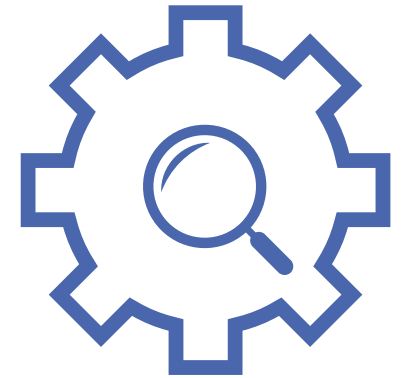


Document search

Only searched
keywords

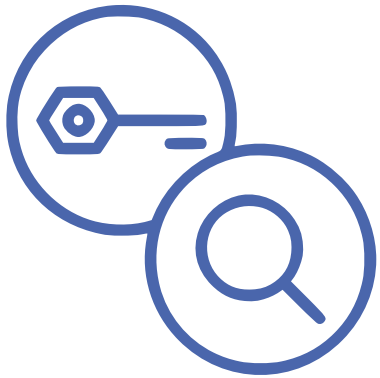


Messaging



DatashareNetwork

Privacy: layers



MS-PSI

Same privacy as
PSI*



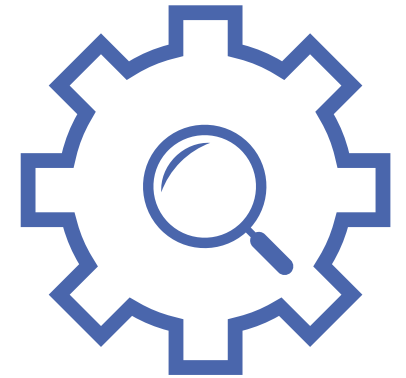
Document search

Only searched
keywords



Messaging

Unobservable



DatashareNetwork

Privacy: layers



MS-PSI

Same privacy as
PSI*



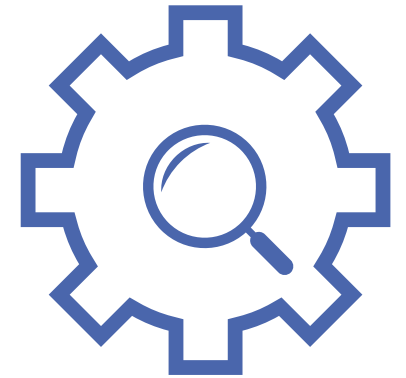
Document search

Only searched
keywords



Messaging

Unobservable



DatashareNetwork

Achieves
privacy goals

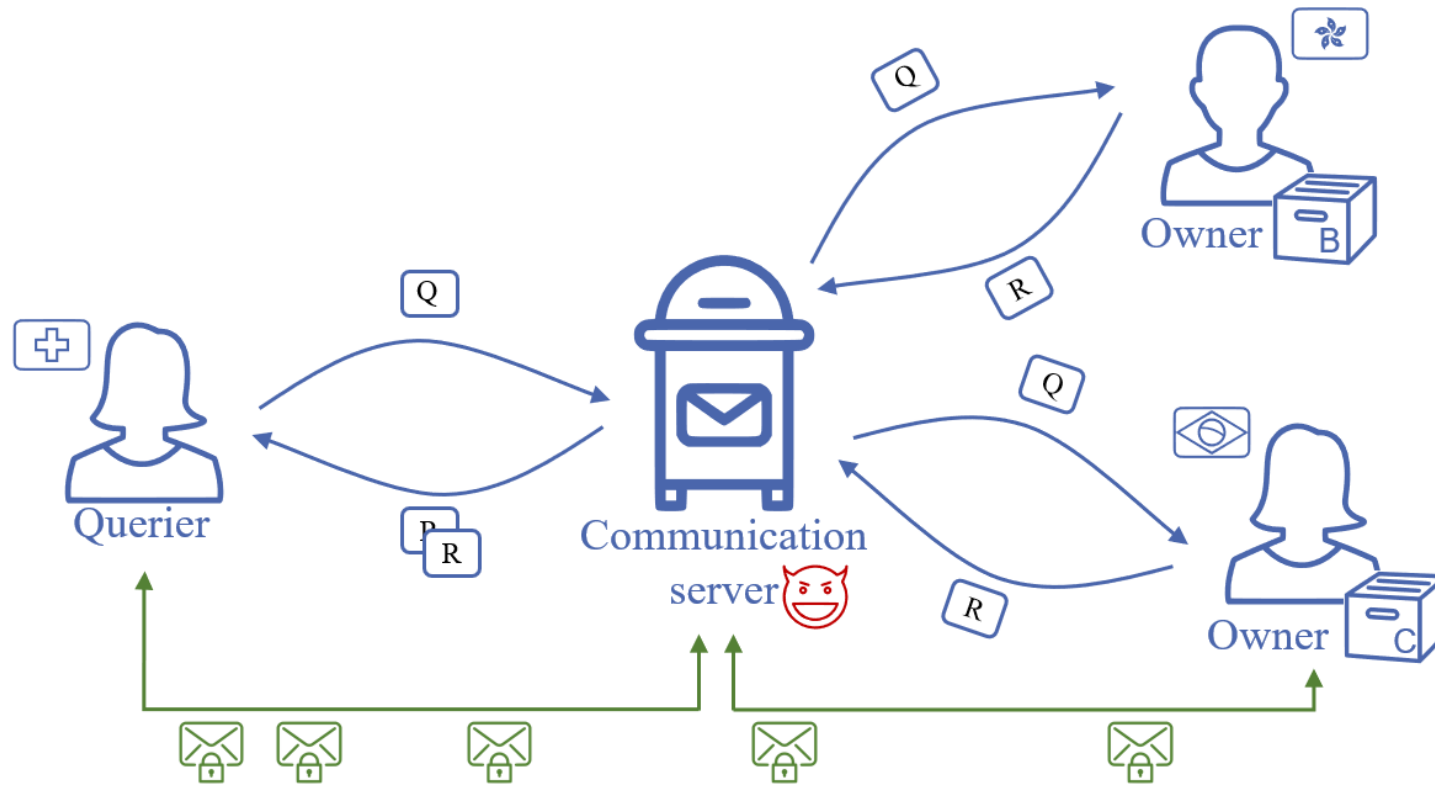
Privacy: a new (stronger) setting



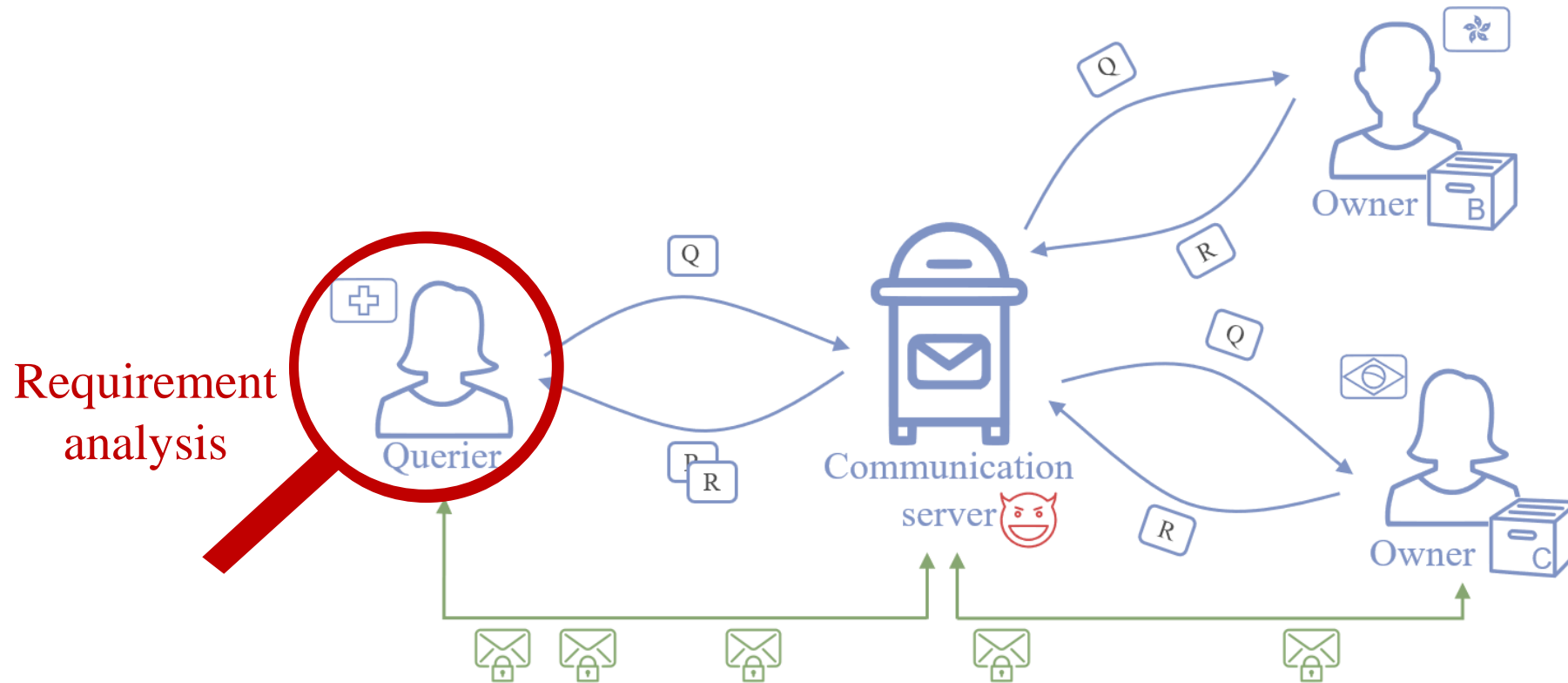
Search access



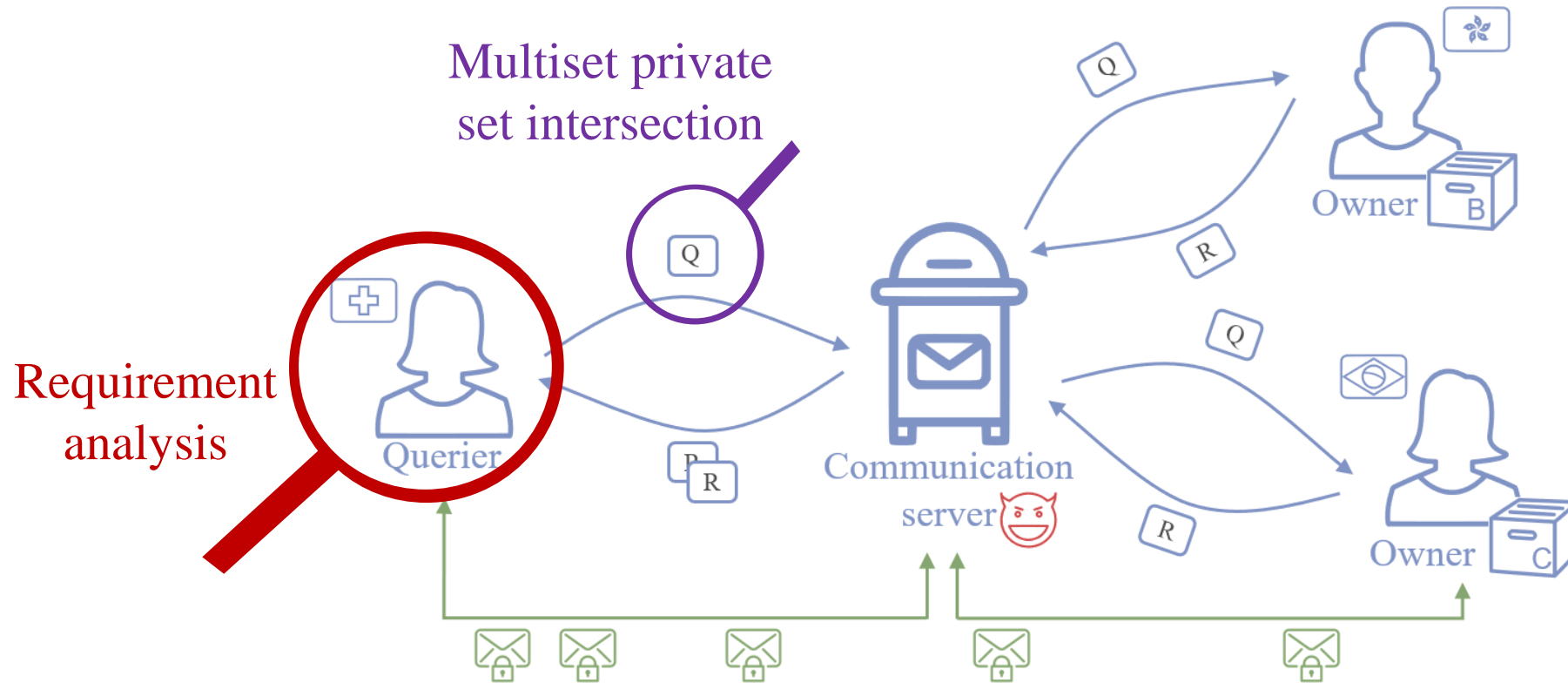
DatashareNetwork



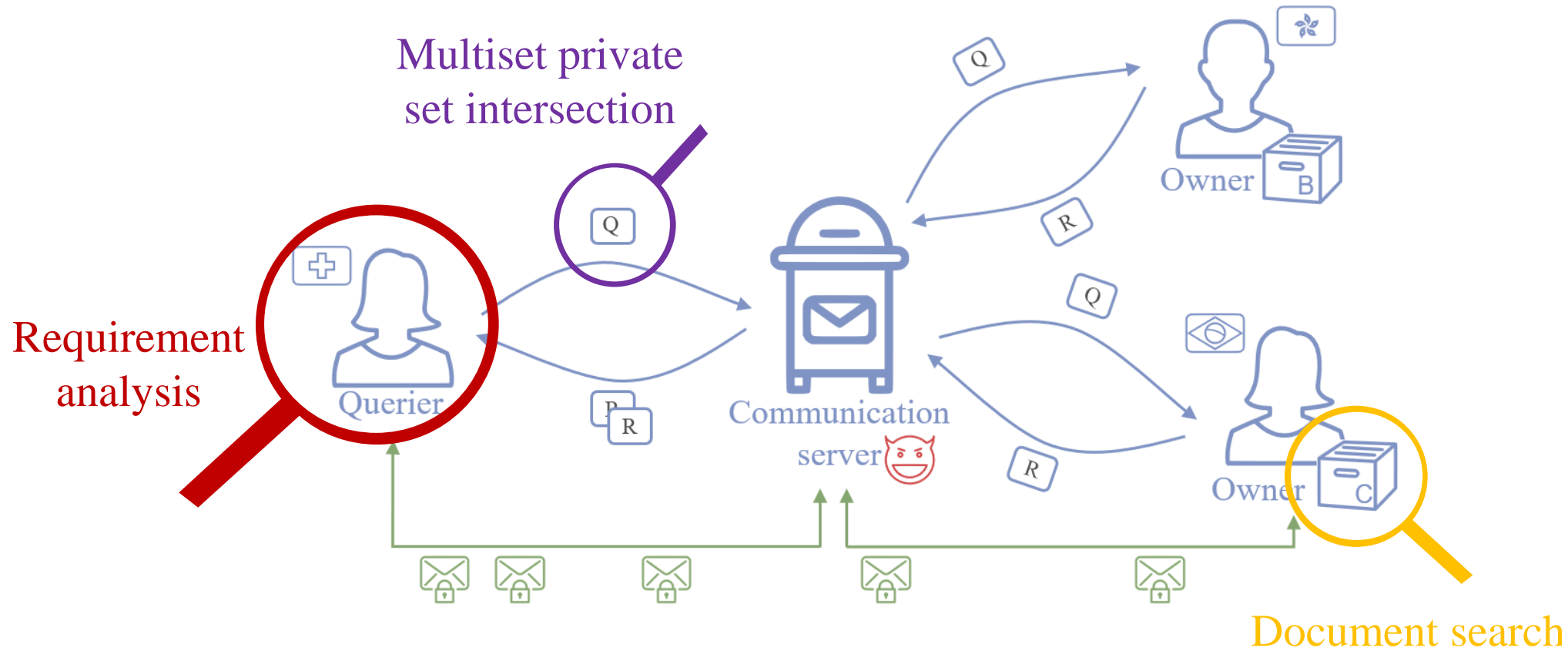
DatashareNetwork



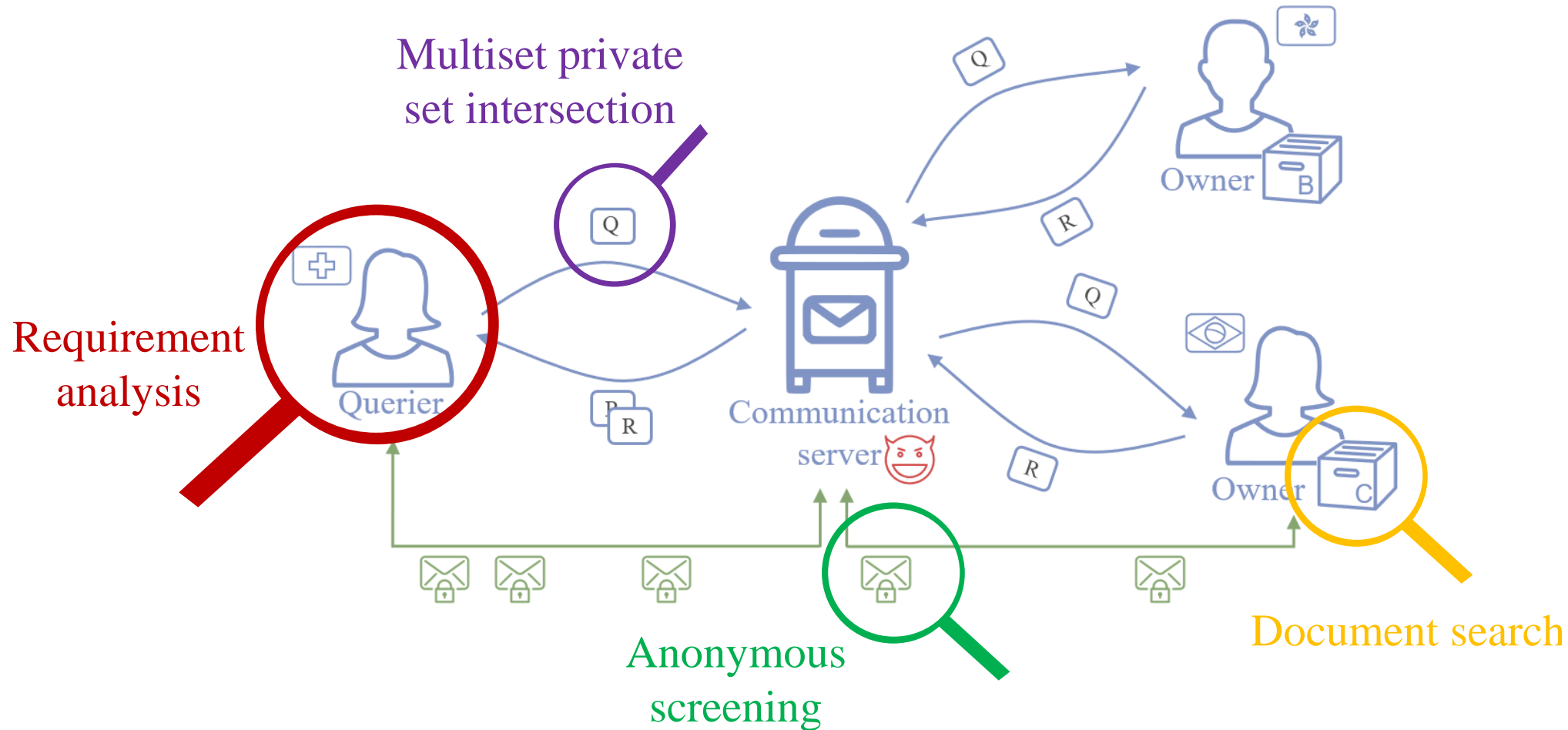
DatashareNetwork



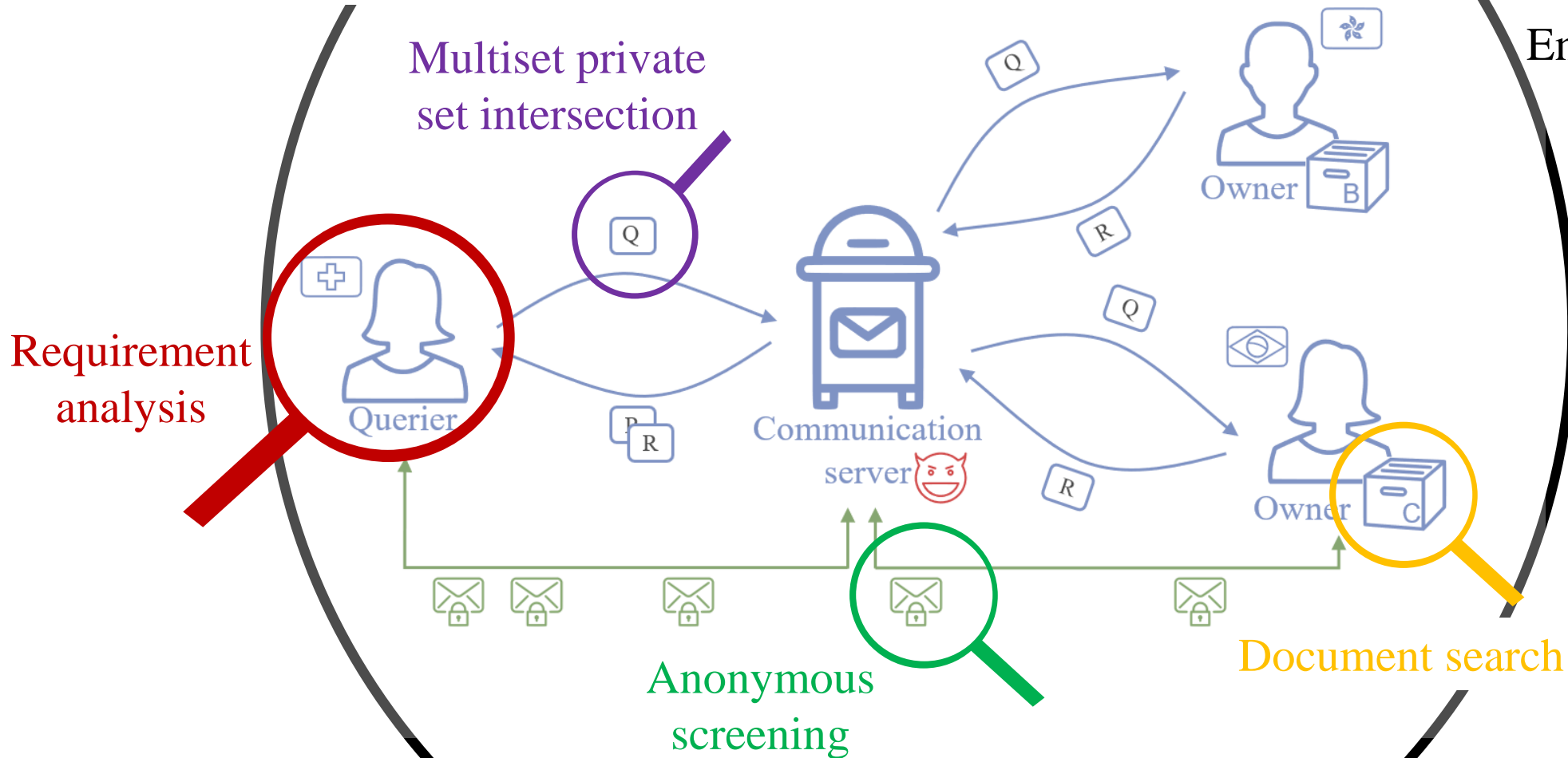
DatashareNetwork



DatashareNetwork



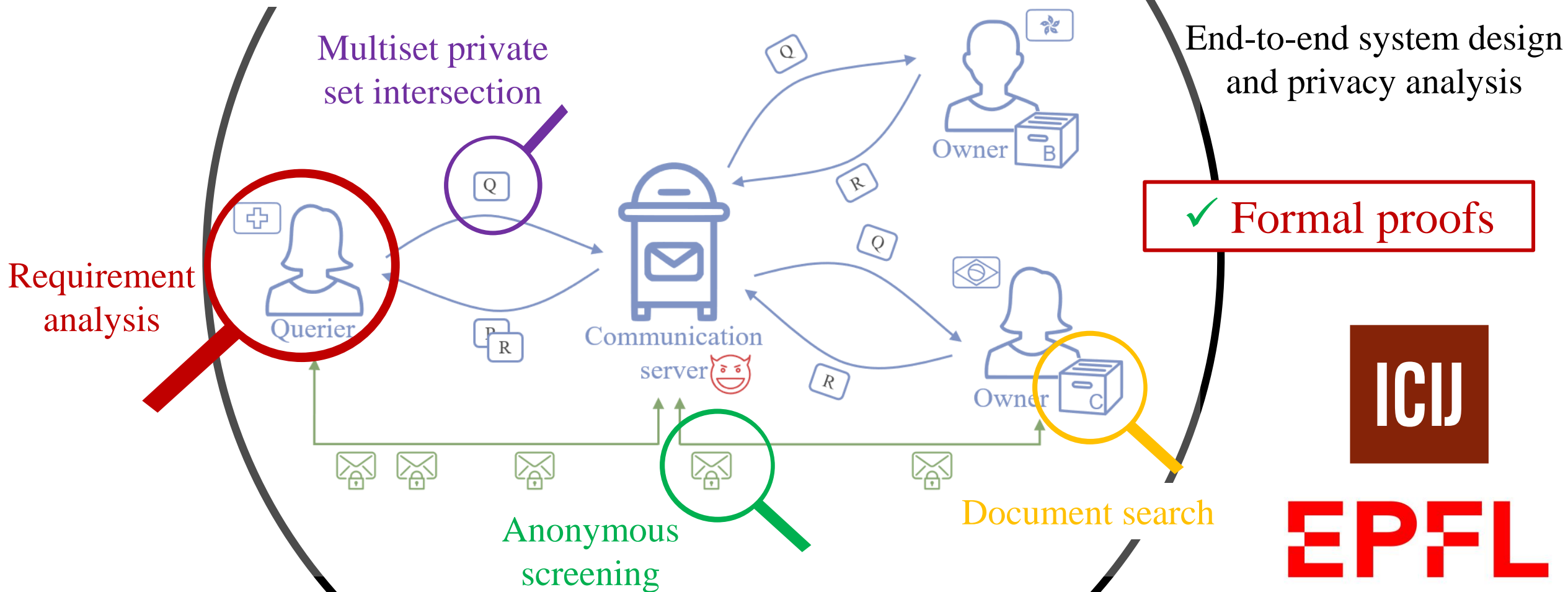
DatashareNetwork



End-to-end system design
and privacy analysis



DatashareNetwork



kasra.edalat@epfl.ch

Thank you for your attention!

