PANCAST: LISTENING TO BLUETOOTH BEACONS FOR EPIDEMIC RISK MITIGATION

Aastha Mehta

Gilles Barthe
MPI For Security And Privacy

Heiner Kremer, Bernhard Schölkopf
MPI For Intelligent Systems

Lars Lorch
ETH Zürich

Matthew Lentz
Duke Univ.

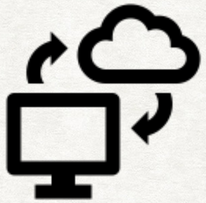
Roberta De Viti, Peter Druschel, Deepak Garg, Manuel Gomez-Rodrigues, Pierfrancesco Ingo
MPI For Software Systems

Nichole Boufford, Ming Cheng-Jiang, Rowan Lindsay
University of British Columbia, Vancouver

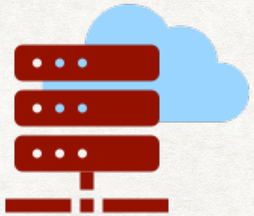
31 AUG 2022

MY RESEARCH

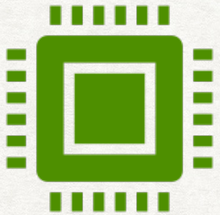
Building systems for security and privacy …



Enabling compliance with data regulations



Mitigating side channels in cloud



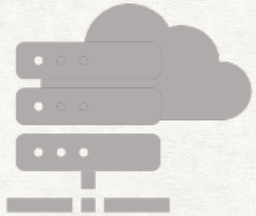
Securing ML in the edge

Inclusive and privacy-preserving contact tracing

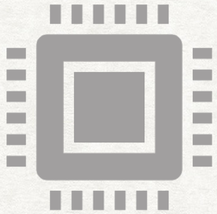
MY RESEARCH

Building systems for security and privacy …

Enabling compliance with data regulations



Mitigating side channels in cloud



Securing ML in the edge

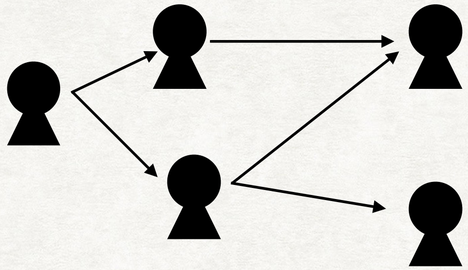
Inclusive and privacy-preserving contact tracing

This talk

KEY STRATEGIES FOR EPIDEMIC MITIGATION

Testing

Contact tracing

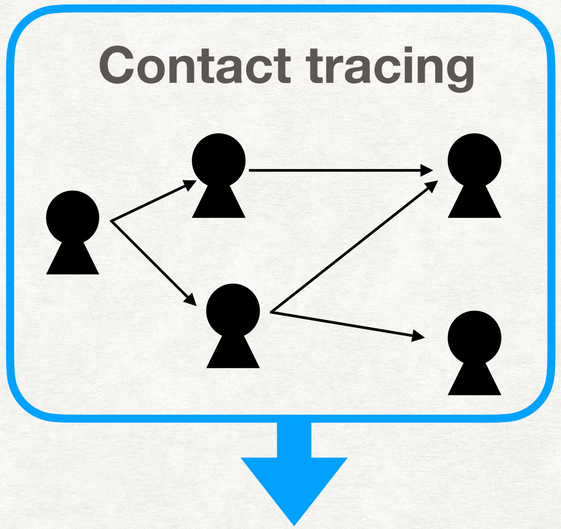


Isolation

KEY STRATEGIES FOR EPIDEMIC MITIGATION

Testing

Contact tracing



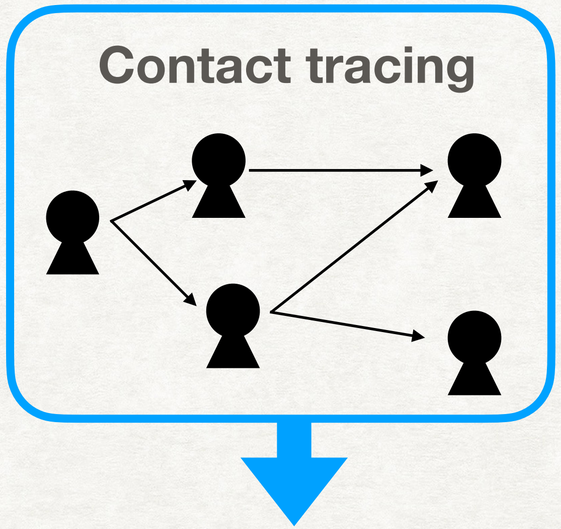
Isolation

Tracing infected persons and those who came in contact with them

KEY STRATEGIES FOR EPIDEMIC MITIGATION

Testing

Contact tracing



Isolation

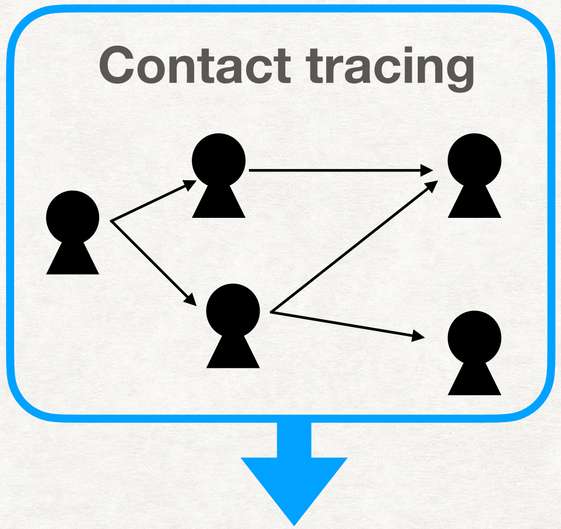
Tracing infected persons and those who came in contact with them

Direct test resources to individuals likely to be infected

KEY STRATEGIES FOR EPIDEMIC MITIGATION

Testing

Contact tracing



Isolation

Tracing infected persons and those who came in contact with them

Direct test resources to individuals likely to be infected

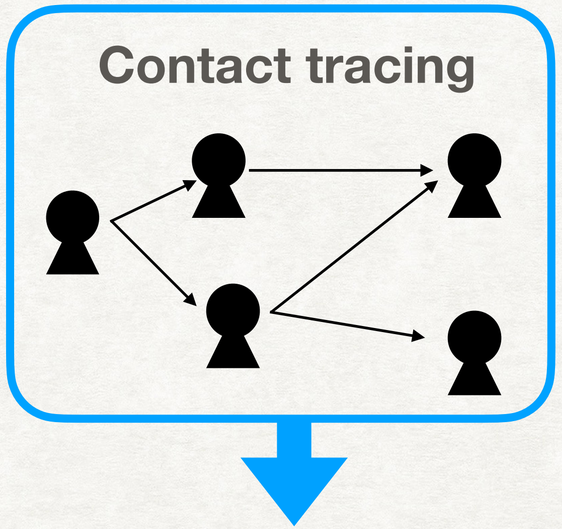
Can provide insights into circumstances of contagion

➡ Inform health policies and interventions that can help contain the disease

KEY STRATEGIES FOR EPIDEMIC MITIGATION

Testing

Contact tracing



Isolation

Tracing infected persons and those who came in contact with them

Direct test resources to individuals likely to be infected

Can provide insights into circumstances of contagion

➡ Inform health policies and interventions that can help contain the disease

More than 1,300 workers test positive: Germany fights to control coronavirus spread at meat plant

The Local
news@thelocal.de
@thelocalgermany

22 June 2020
11:32 CEST

Updated
22 June 2020
17:11 CEST

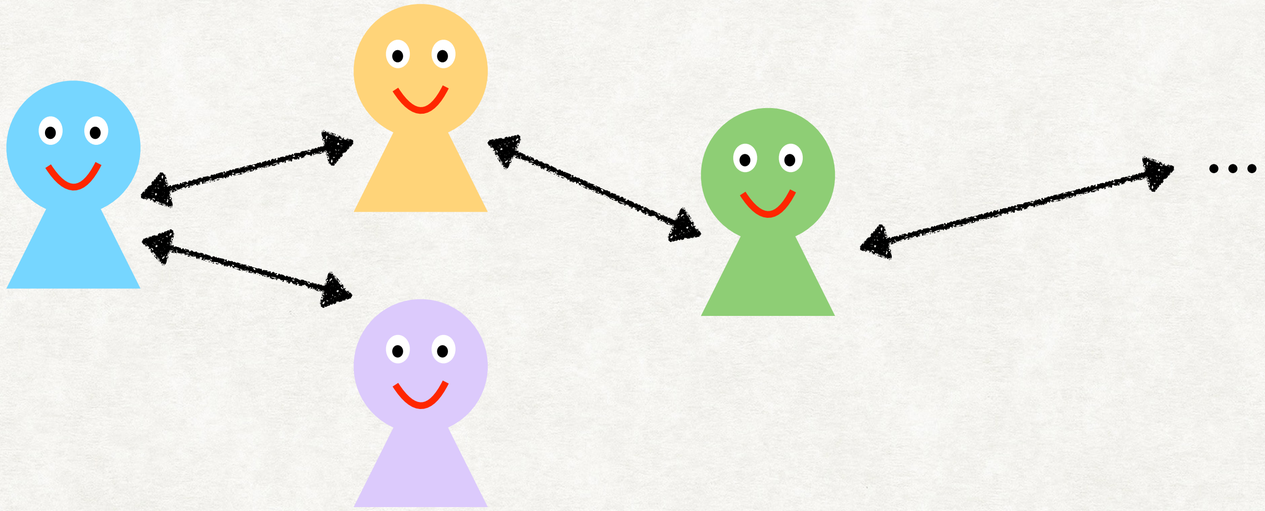
coronavirus
industry
meat

Share this article

Members of the Bundeswehr (German Army) outside Tönnies. Photo: DPA

MANUAL CONTACT TRACING

Health workers interview sick persons about their recent encounters and travel history

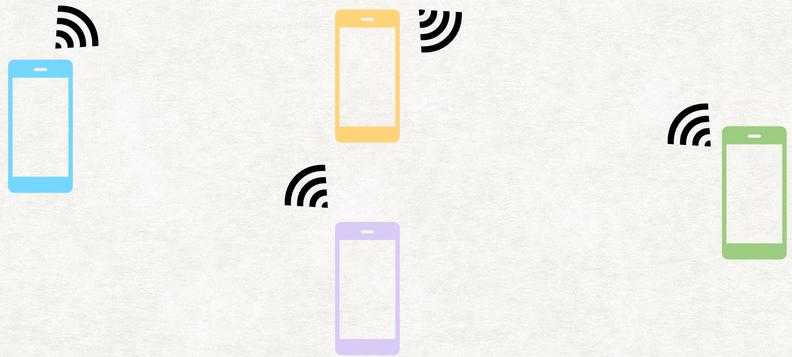


Limitations

- Difficult to scale
- People forget information

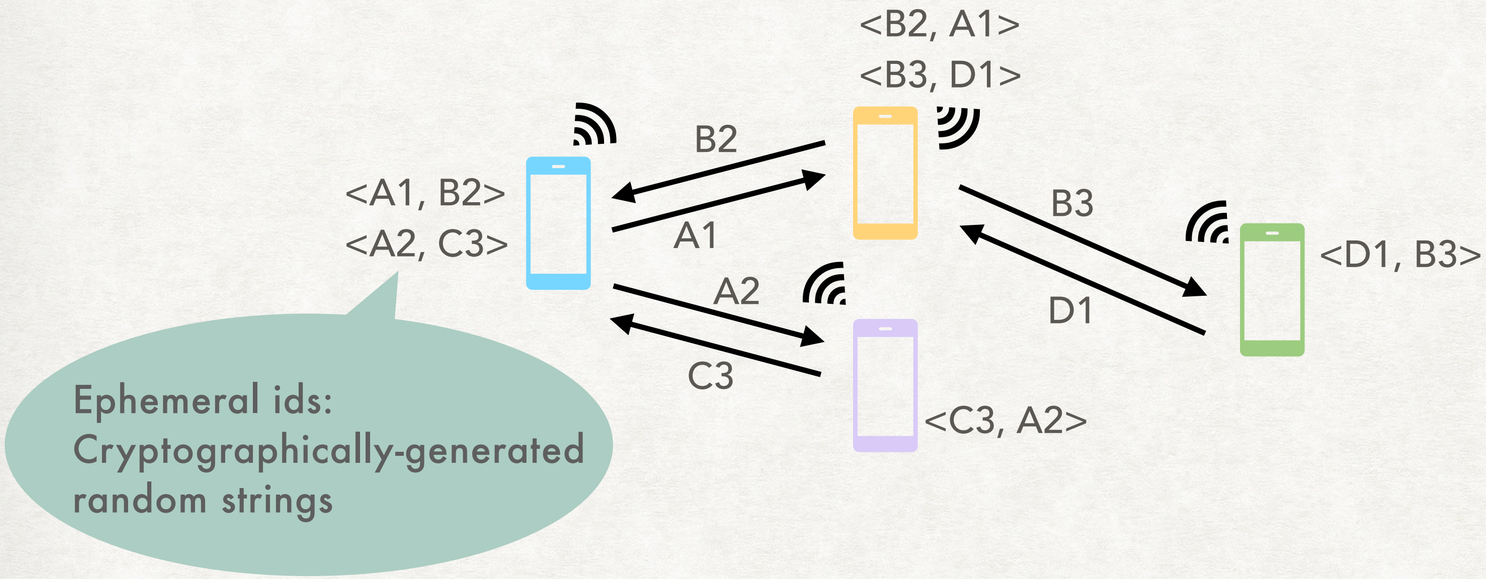
DIGITAL CONTACT TRACING

SPECTS: **S**martphone-**B**ased **P**airwise **E**ncounter-Based **C**ontact **T**racing **S**ystems



DIGITAL CONTACT TRACING

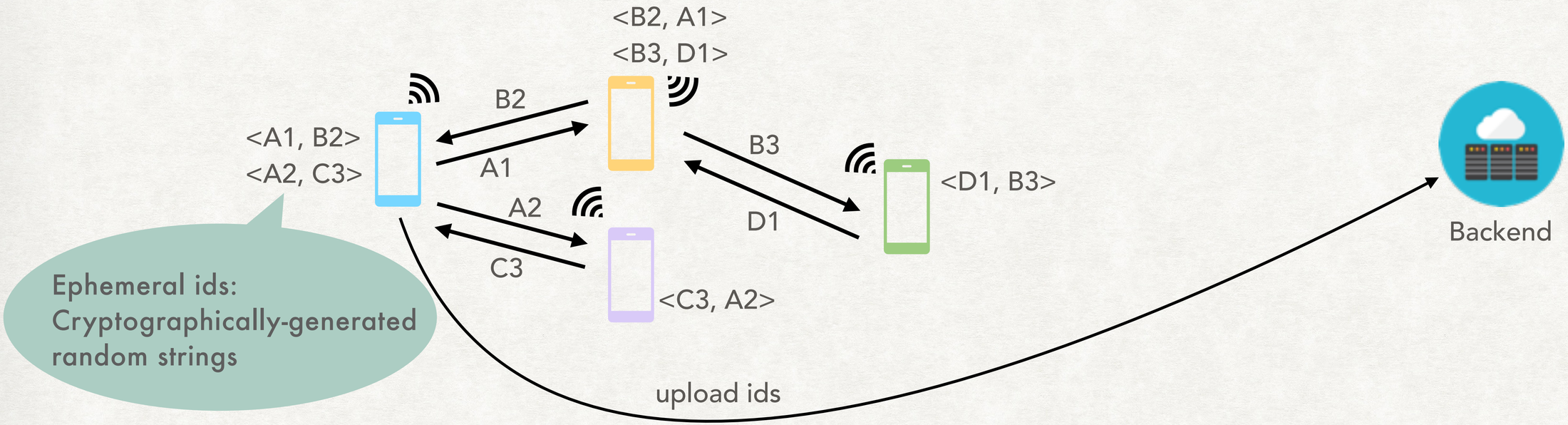
SPECTS: **S**martphone-**B**ased **P**airwise **E**ncounter-Based **C**ontact **T**racing **S**ystems



- Record physical proximity between users via close-range bluetooth exchange

DIGITAL CONTACT TRACING

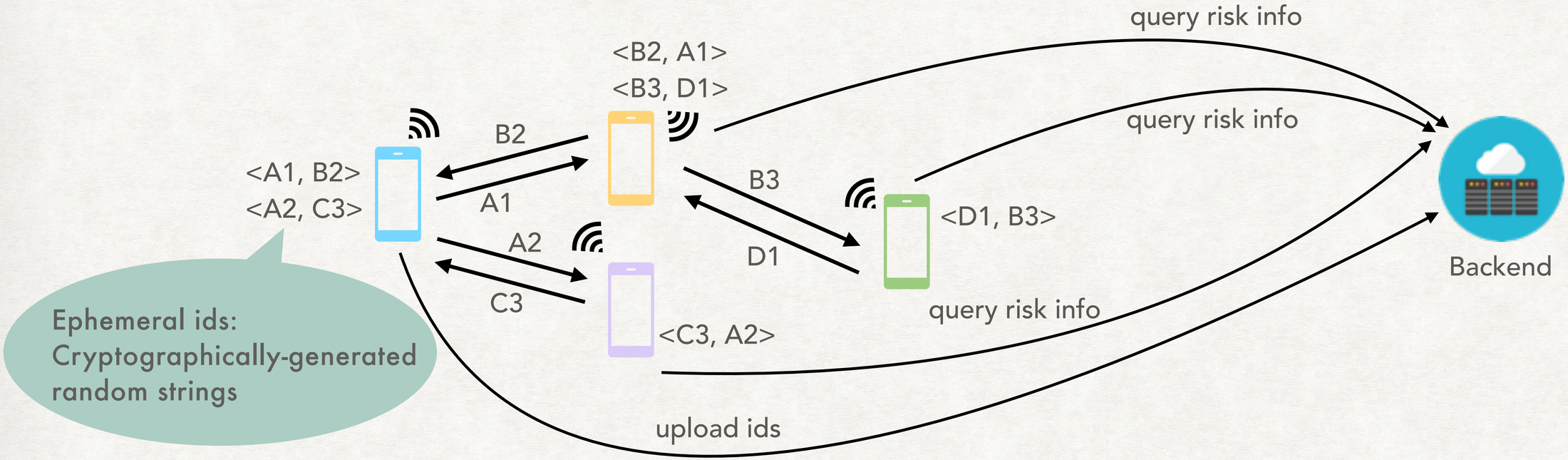
SPECTS: **S**martphone-**B**ased **P**airwise **E**ncounter-Based **C**ontact **T**racing **S**ystems



- Record physical proximity between users via close-range bluetooth exchange
- Sick persons report encounter history to a health authority (backend)

DIGITAL CONTACT TRACING

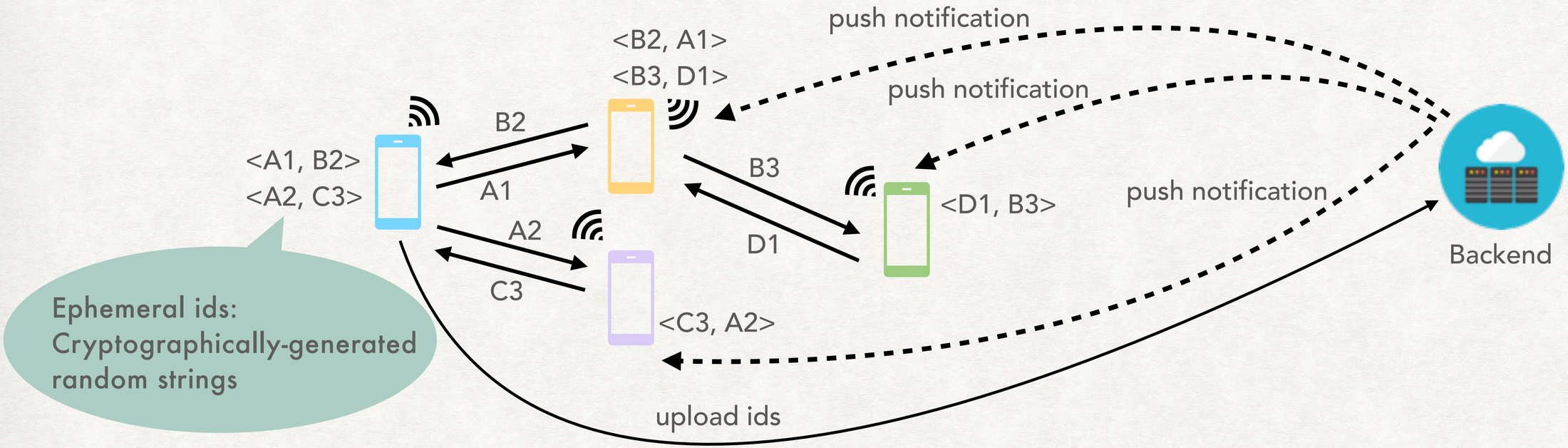
SPECTS: **S**martphone-**B**ased **P**airwise **E**ncounter-Based **C**ontact **T**racing **S**ystems



- Record physical proximity between users via close-range bluetooth exchange
- Sick persons report encounter history to a health authority (backend)
- Users query backend for risk info (centralized) OR

DIGITAL CONTACT TRACING

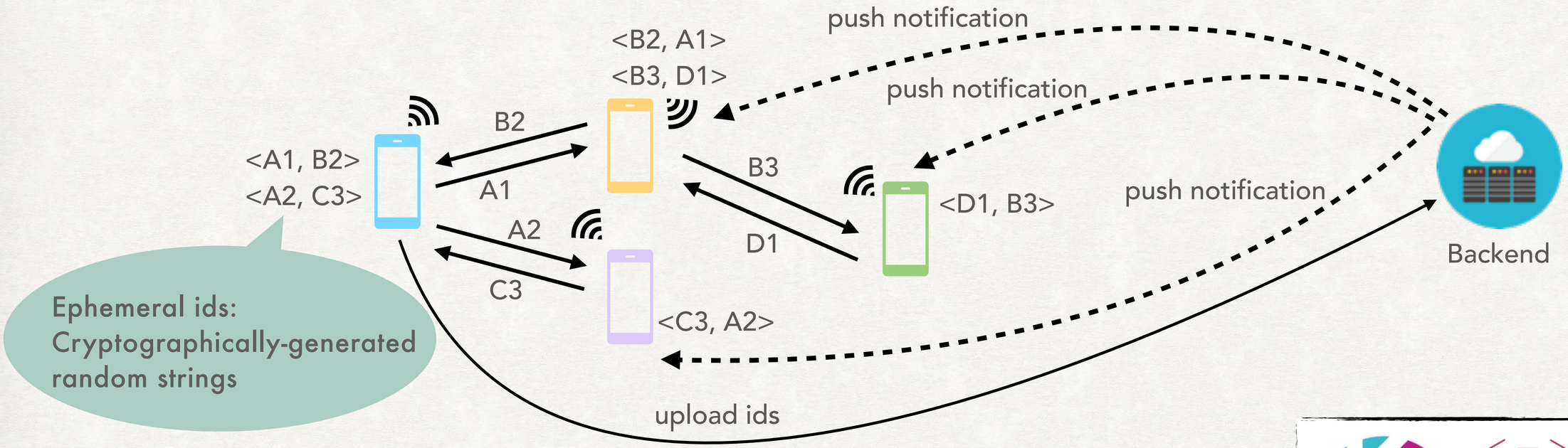
SPECTS: **S**martphone-**B**ased **P**airwise **E**ncounter-Based **C**ontact **T**racing **S**ystems



- Record physical proximity between users via close-range bluetooth exchange
- Sick persons report encounter history to a health authority (backend)
- Users query backend for risk info (centralized) OR
- Backend notifies users (decentralized)

DIGITAL CONTACT TRACING

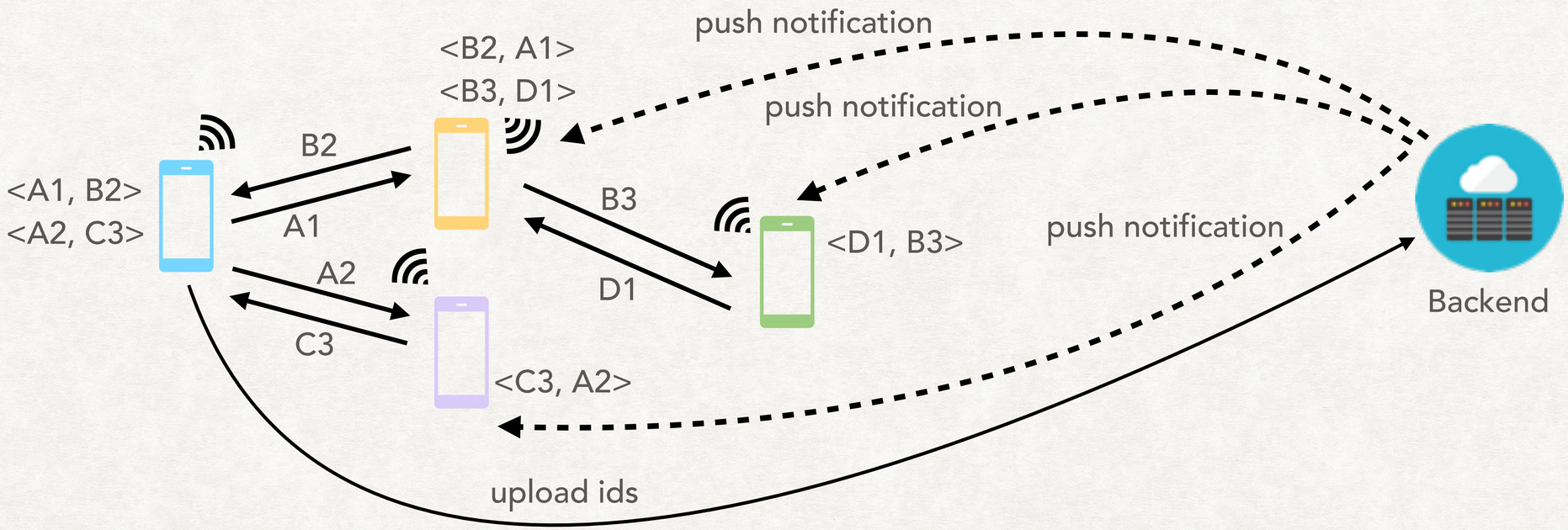
SPECTS: **S**martphone-**B**ased **P**airwise **E**ncounter-Based **C**ontact **T**racing **S**ystems



- Record physical proximity between users via close-range bluetooth exchange
- Sick persons report encounter history to a health authority (backend)
- Users query backend for risk info (centralized) OR
- Backend notifies users (decentralized)

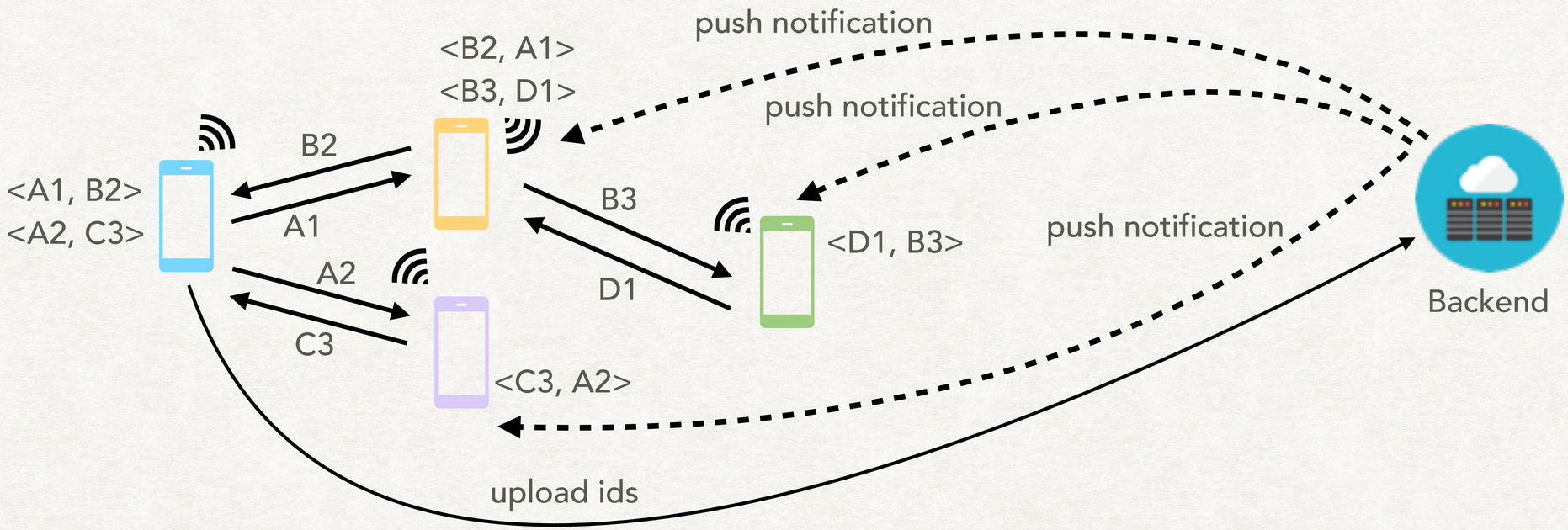
Logos courtesy: wikipedia.org, wikimedia.org

LIMITED EFFECTIVENESS OF CURRENT SPECTS



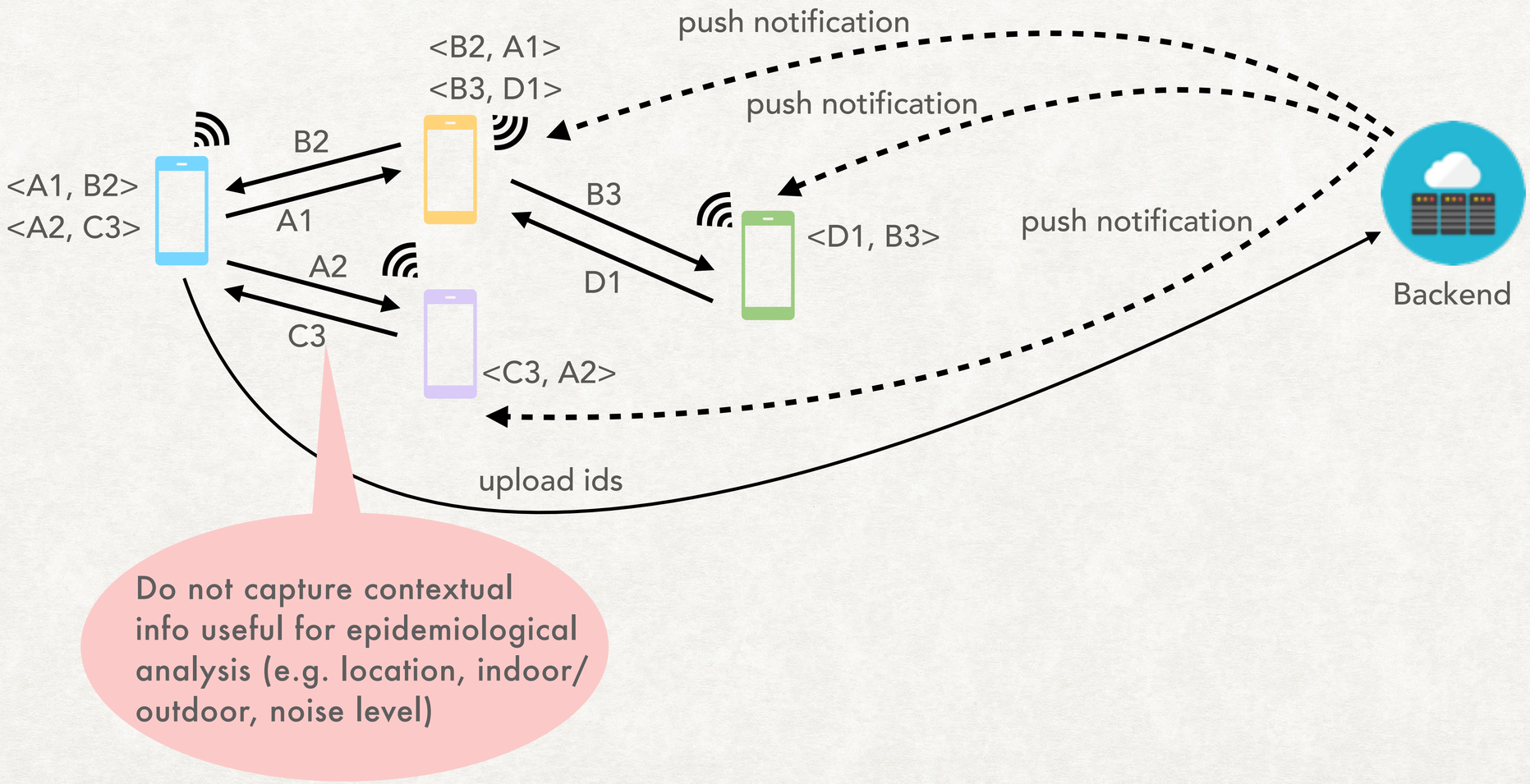
LIMITED EFFECTIVENESS OF CURRENT SPECTS

Trade utility for privacy



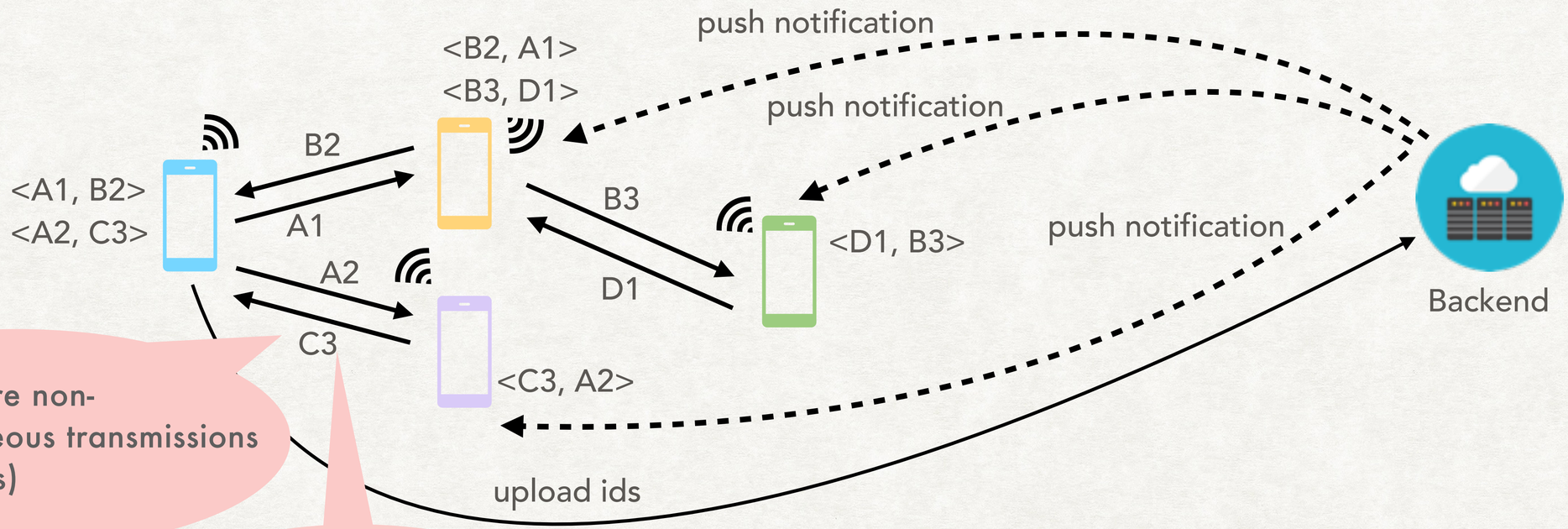
LIMITED EFFECTIVENESS OF CURRENT SPECTS

Trade utility for privacy



LIMITED EFFECTIVENESS OF CURRENT SPECTS

Trade utility for privacy

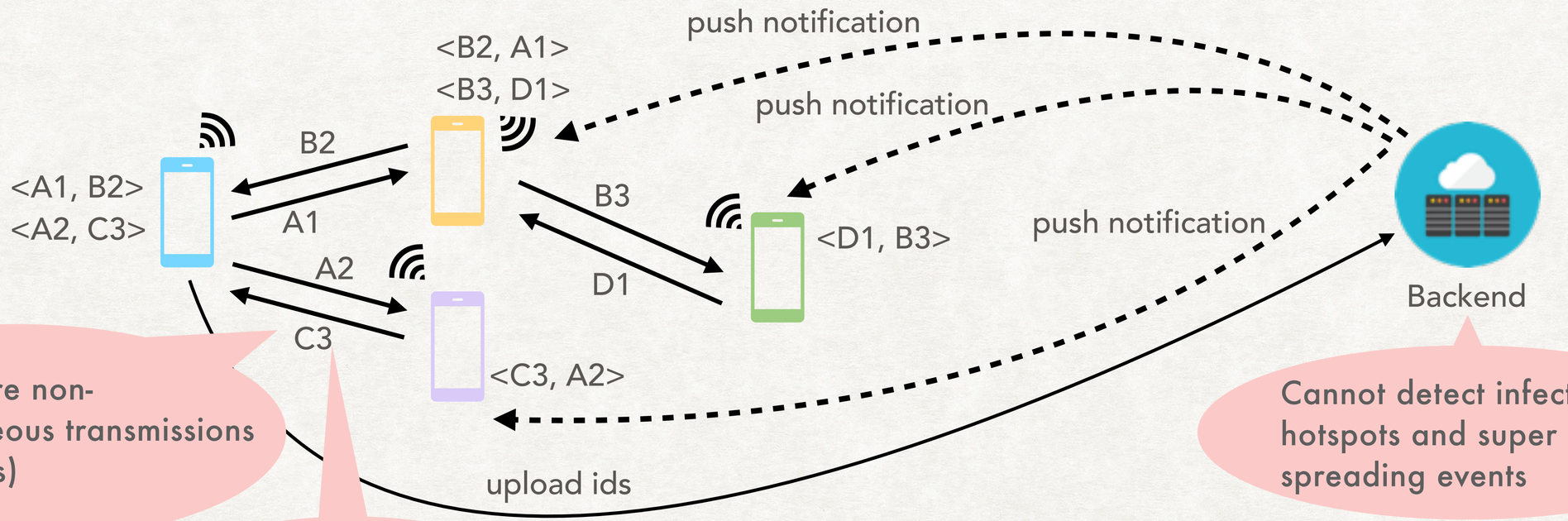


Cannot capture non-contemporaneous transmissions (e.g. elevators)

Do not capture contextual info useful for epidemiological analysis (e.g. location, indoor/ outdoor, noise level)

LIMITED EFFECTIVENESS OF CURRENT SPECTS

Trade utility for privacy



Cannot capture non-contemporaneous transmissions (e.g. elevators)

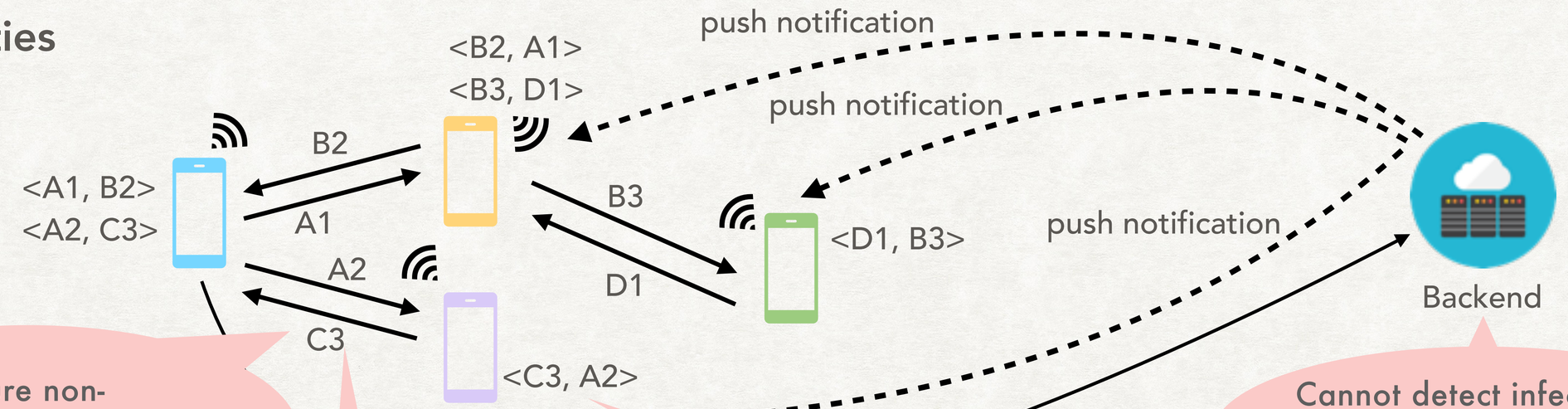
Do not capture contextual info useful for epidemiological analysis (e.g. location, indoor/ outdoor, noise level)

Cannot detect infection hotspots and super spreading events

LIMITED EFFECTIVENESS OF CURRENT SPECTS

Trade utility for privacy

Vulnerabilities



Cannot capture non-contemporaneous transmissions (e.g. elevators)

Do not capture contextual info useful for epidemiological analysis (e.g. location, indoor/ outdoor, noise level)

Vulnerable to eavesdropping, relay and replay attacks

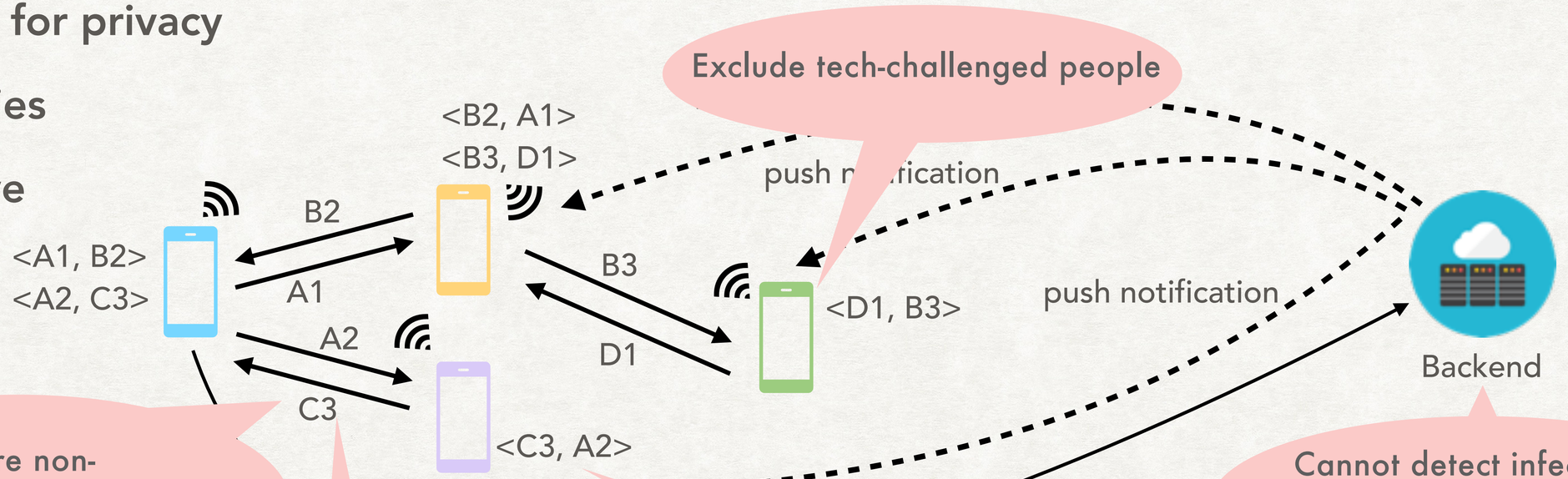
Cannot detect infection hotspots and super spreading events

LIMITED EFFECTIVENESS OF CURRENT SPECTS

Trade utility for privacy

Vulnerabilities

Non-inclusive



Exclude tech-challenged people

Cannot capture non-contemporaneous transmissions (e.g. elevators)

Do not capture contextual info useful for epidemiological analysis (e.g. location, indoor/ outdoor, noise level)

Vulnerable to eavesdropping, relay and replay attacks

Cannot detect infection hotspots and super spreading events

PANCAST: INCLUSIVE, PRIVACY-PRESERVING, SCALABLE

Key Primitive: Infrastructure-to-User Encounters

PANCAST: INCLUSIVE, PRIVACY-PRESERVING, SCALABLE

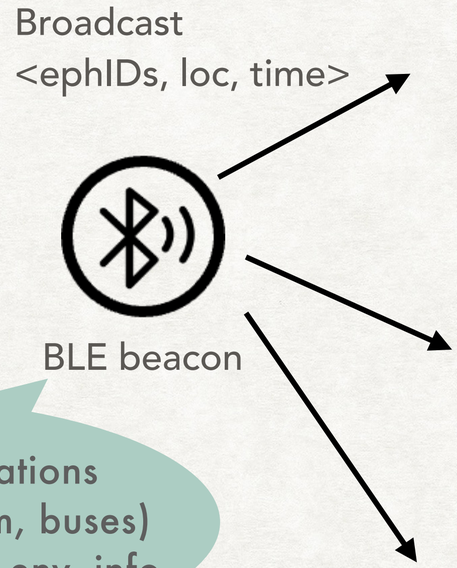
Key Primitive: Infrastructure-to-User Encounters

BLE beacon

- Placed in strategic locations (restaurants, classroom, buses)
- Labeled with location, env. info

PANCAST: INCLUSIVE, PRIVACY-PRESERVING, SCALABLE

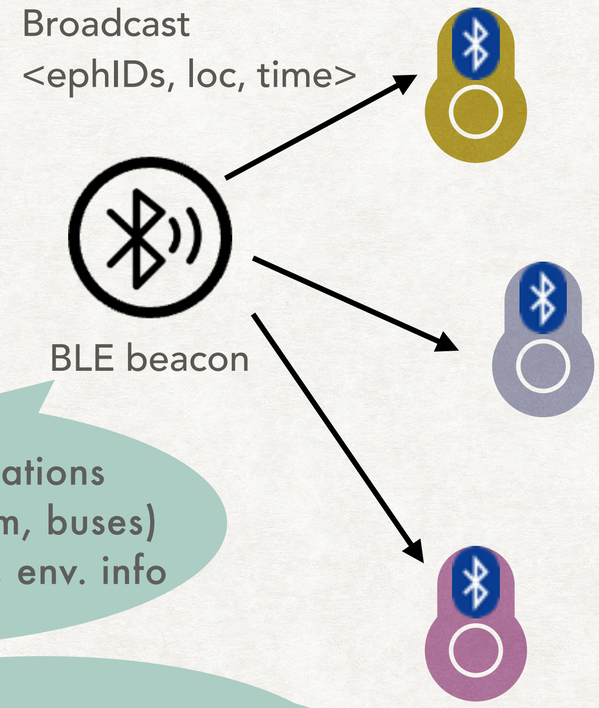
Key Primitive: Infrastructure-to-User Encounters



- Placed in strategic locations (restaurants, classroom, buses)
- Labeled with location, env. info

PANCAST: INCLUSIVE, PRIVACY-PRESERVING, SCALABLE

Key Primitive: Infrastructure-to-User Encounters

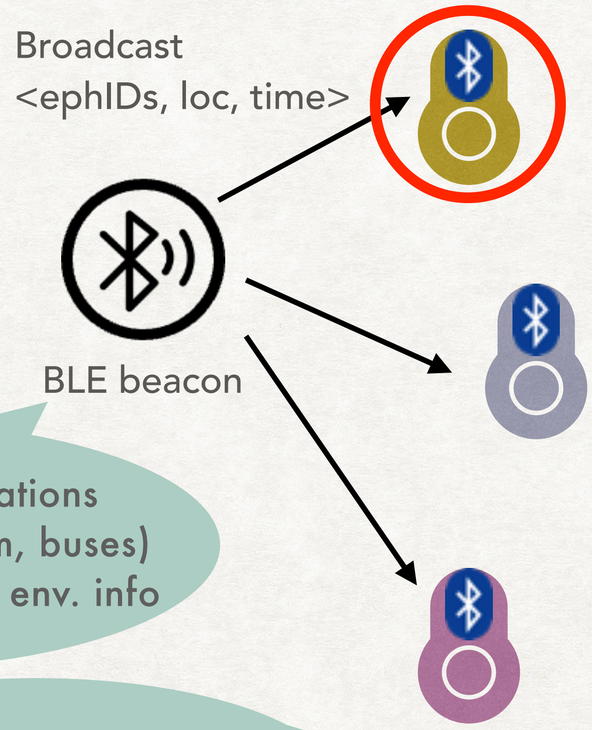


- Placed in strategic locations (restaurants, classroom, buses)
- Labeled with location, env. info

- Low cost, zero-maintenance
- Simple button, LED interface

PANCAST: INCLUSIVE, PRIVACY-PRESERVING, SCALABLE

Key Primitive: Infrastructure-to-User Encounters

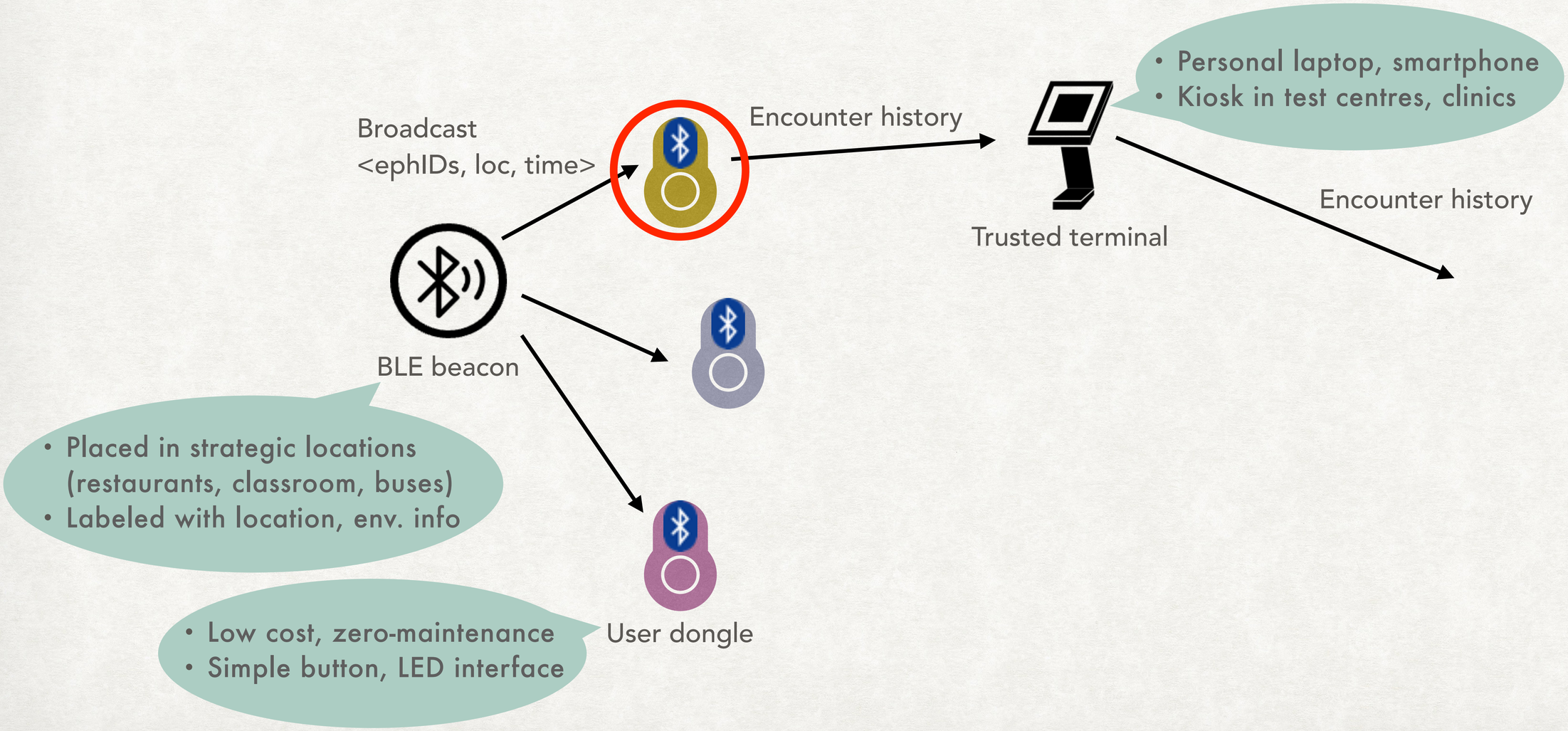


- Placed in strategic locations (restaurants, classroom, buses)
- Labeled with location, env. info

- Low cost, zero-maintenance
- Simple button, LED interface

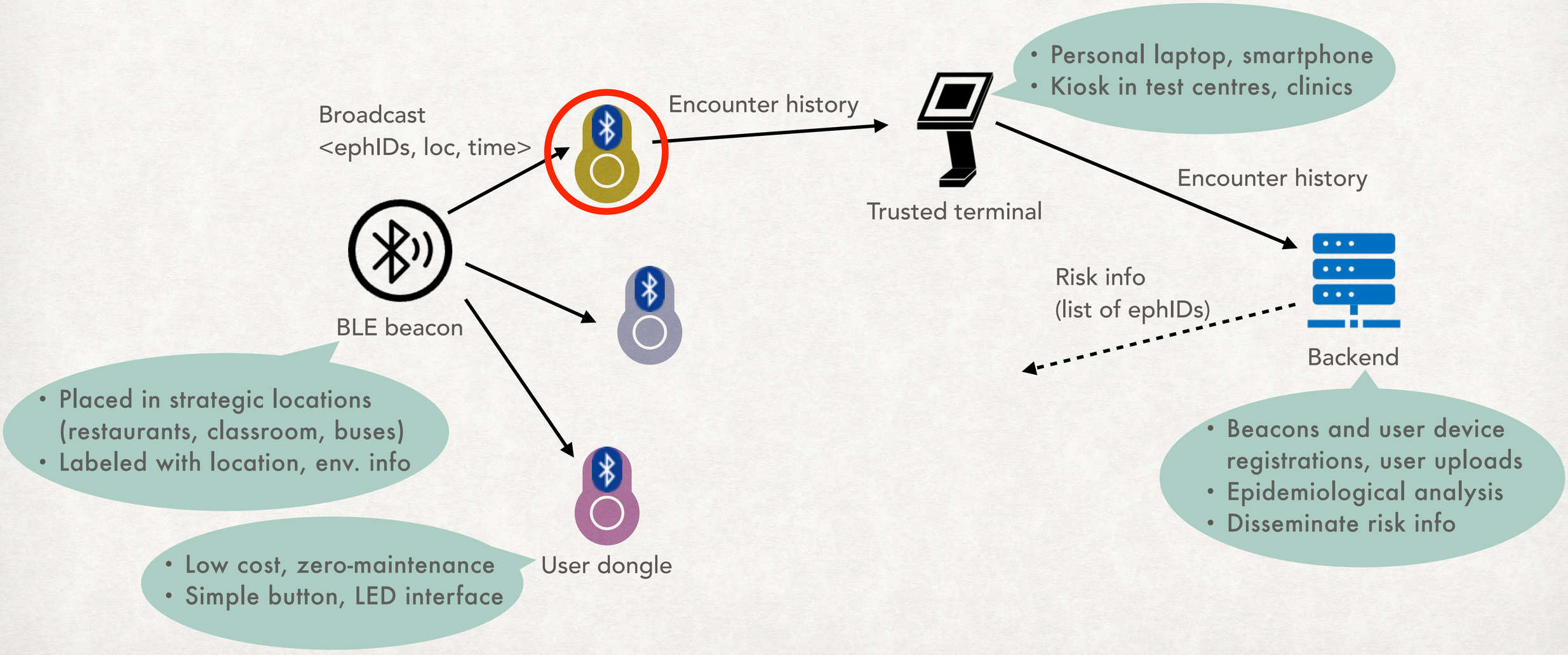
PANCAST: INCLUSIVE, PRIVACY-PRESERVING, SCALABLE

Key Primitive: Infrastructure-to-User Encounters



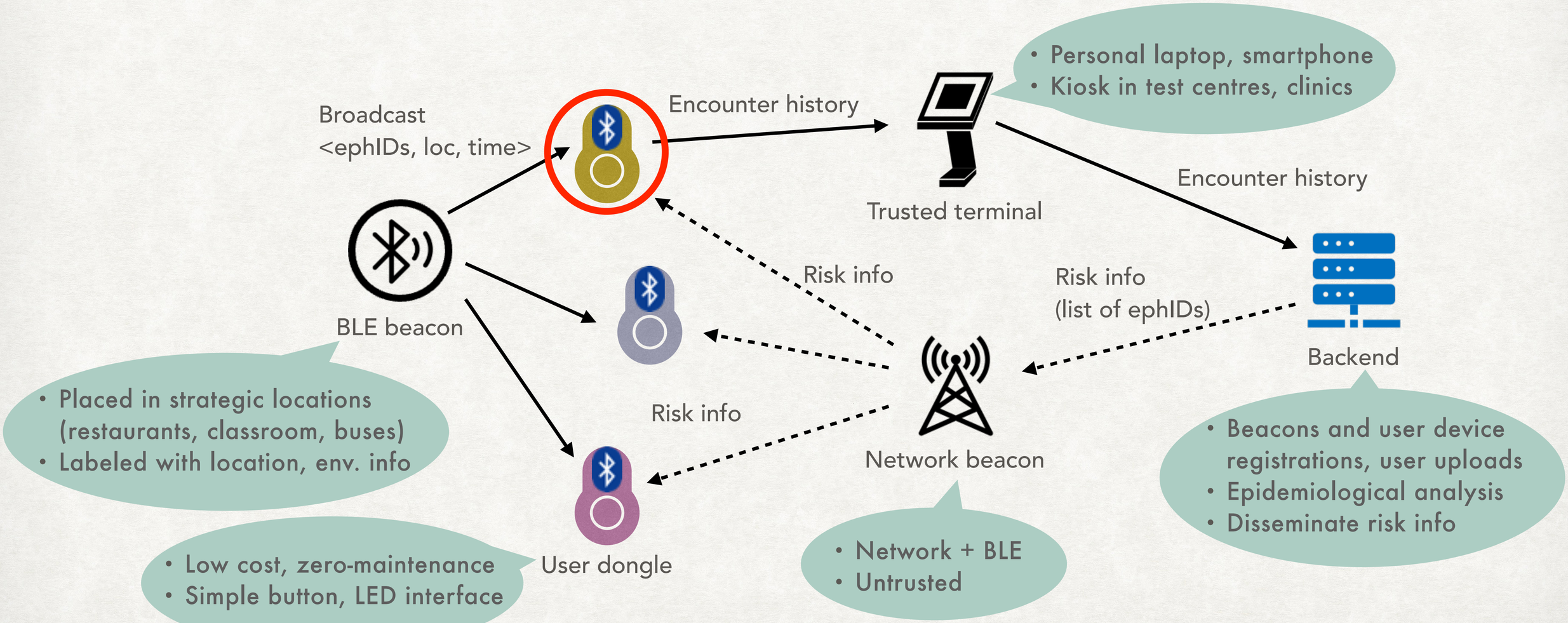
PANCAST: INCLUSIVE, PRIVACY-PRESERVING, SCALABLE

Key Primitive: Infrastructure-to-User Encounters



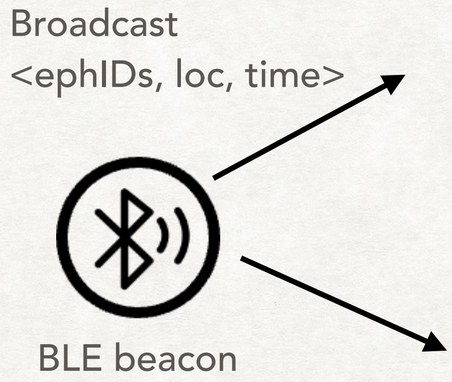
PANCAST: INCLUSIVE, PRIVACY-PRESERVING, SCALABLE

Key Primitive: Infrastructure-to-User Encounters



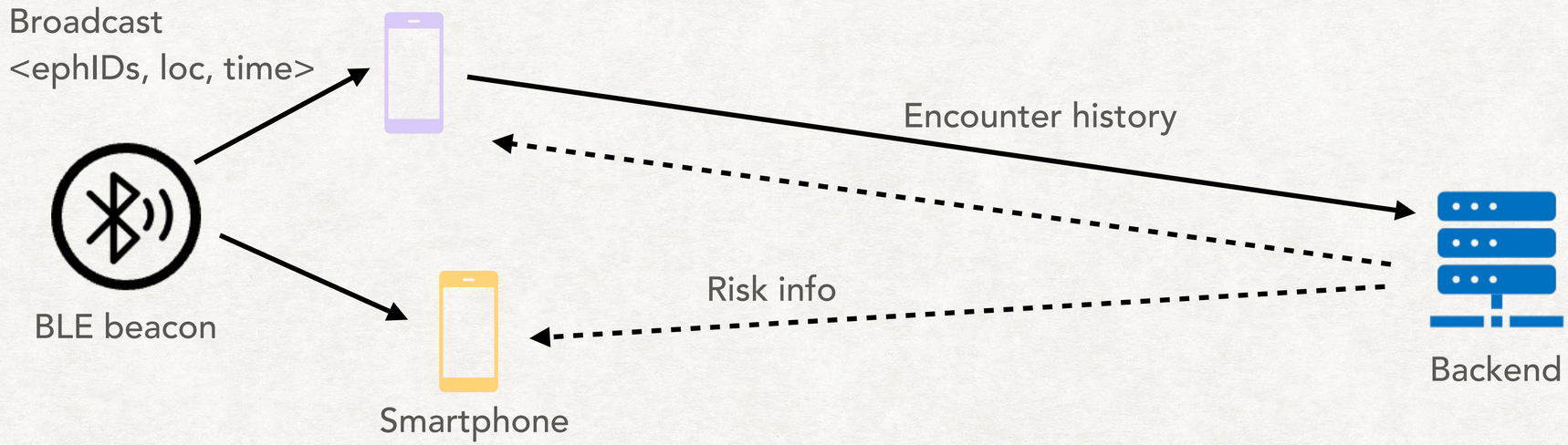
PANCAST: INCLUSIVE, PRIVACY-PRESERVING, SCALABLE

Key Primitive: Infrastructure-to-User Encounters



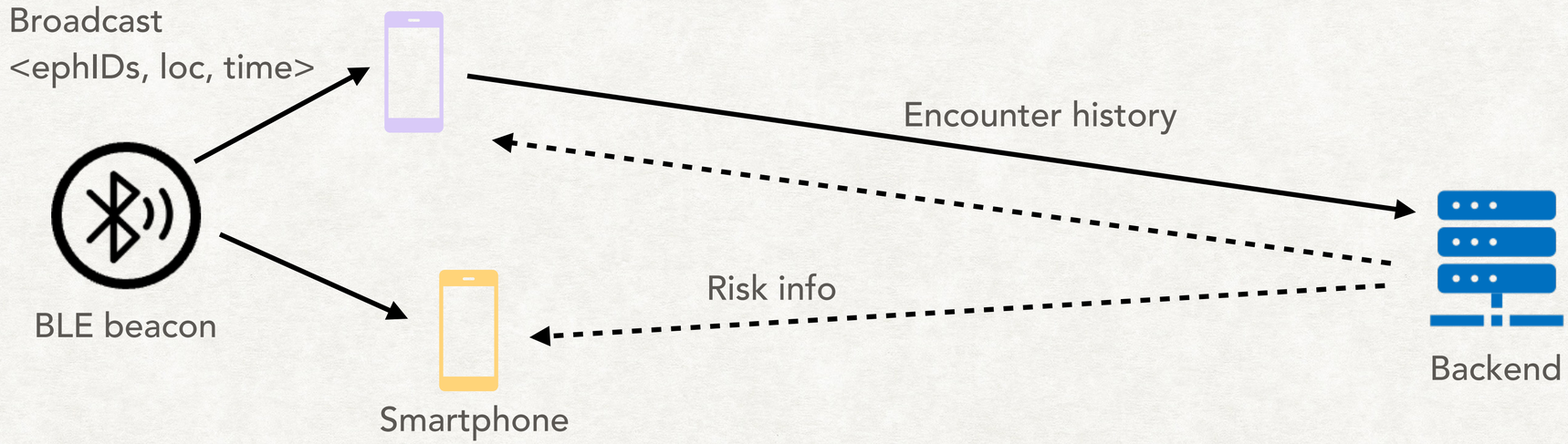
PANCAST: INCLUSIVE, PRIVACY-PRESERVING, SCALABLE

Key Primitive: Infrastructure-to-User Encounters



PANCAST: INCLUSIVE, PRIVACY-PRESERVING, SCALABLE

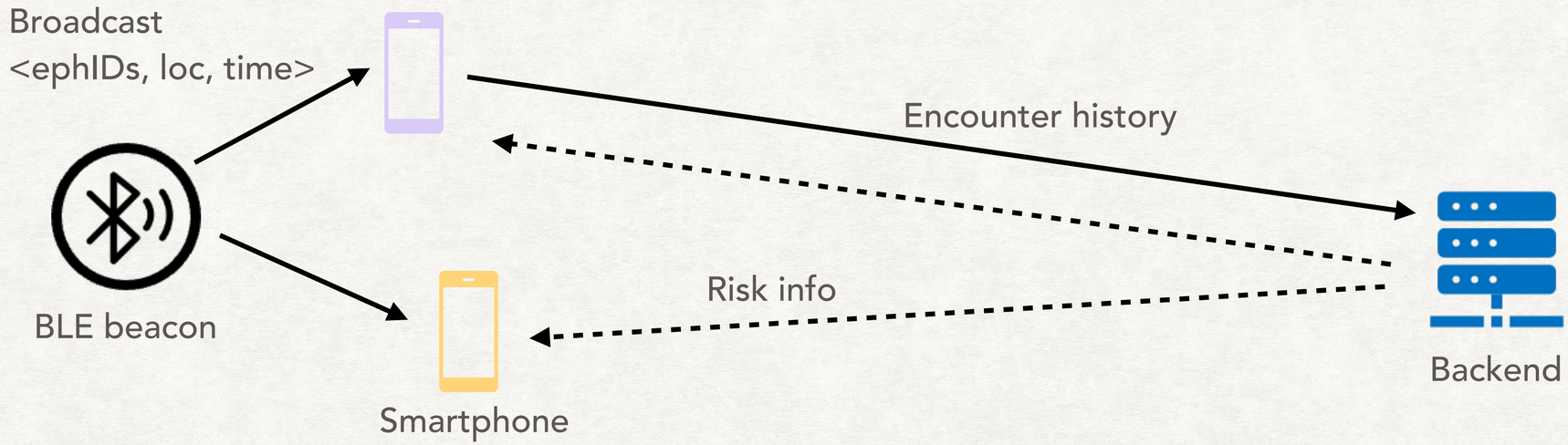
Key Primitive: Infrastructure-to-User Encounters



- User devices mostly passive
- Transmit with explicit user consent
- Decentralized risk notification

PANCAST: INCLUSIVE, PRIVACY-PRESERVING, SCALABLE

Key Primitive: Infrastructure-to-User Encounters



- User devices mostly passive
- Transmit with explicit user consent
- Decentralized risk notification

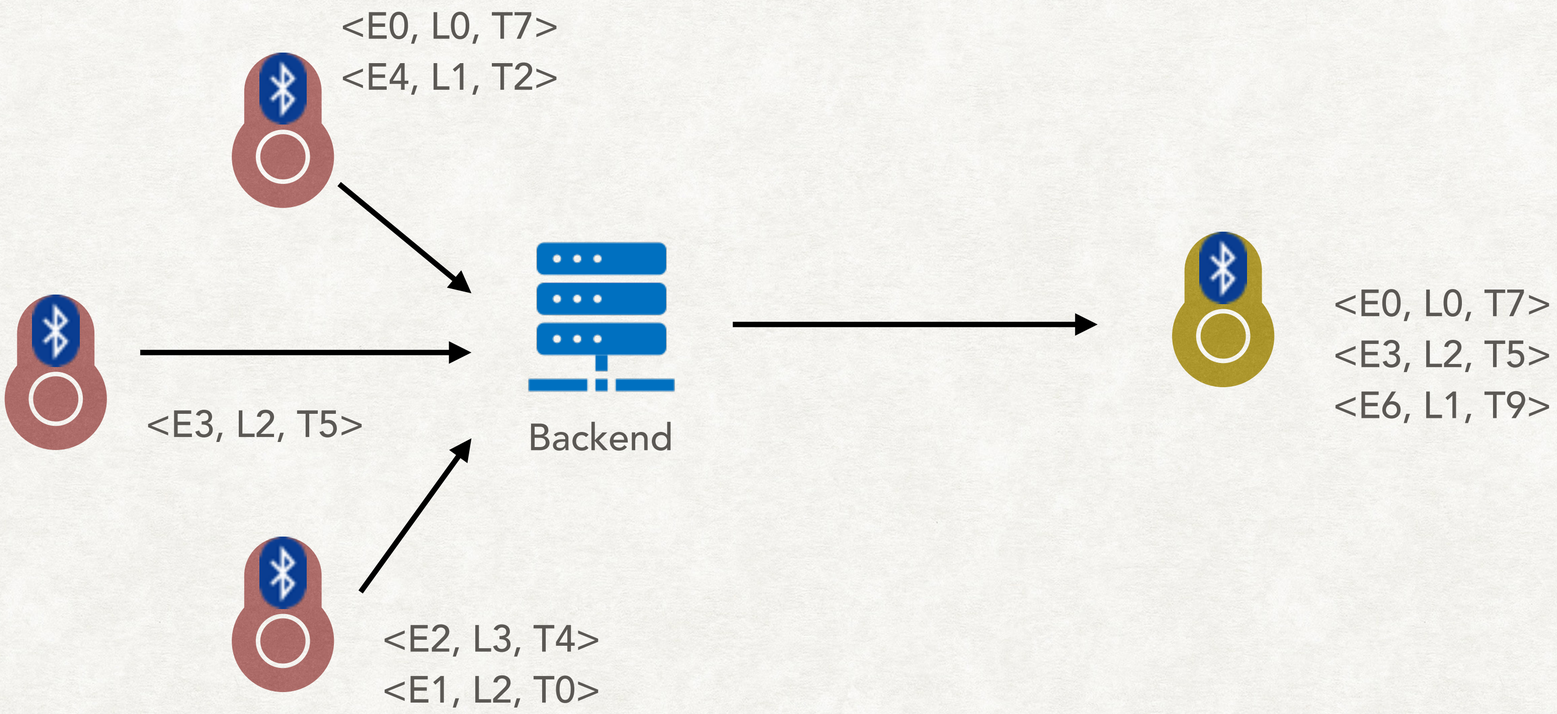
- Minimizes data collection
- Similar privacy as existing SPECTS while using location info
- Robust against eavesdropping, relay, and replay attacks

OUTLINE

- Risk dissemination
- Implementation and evaluation
- Deployment

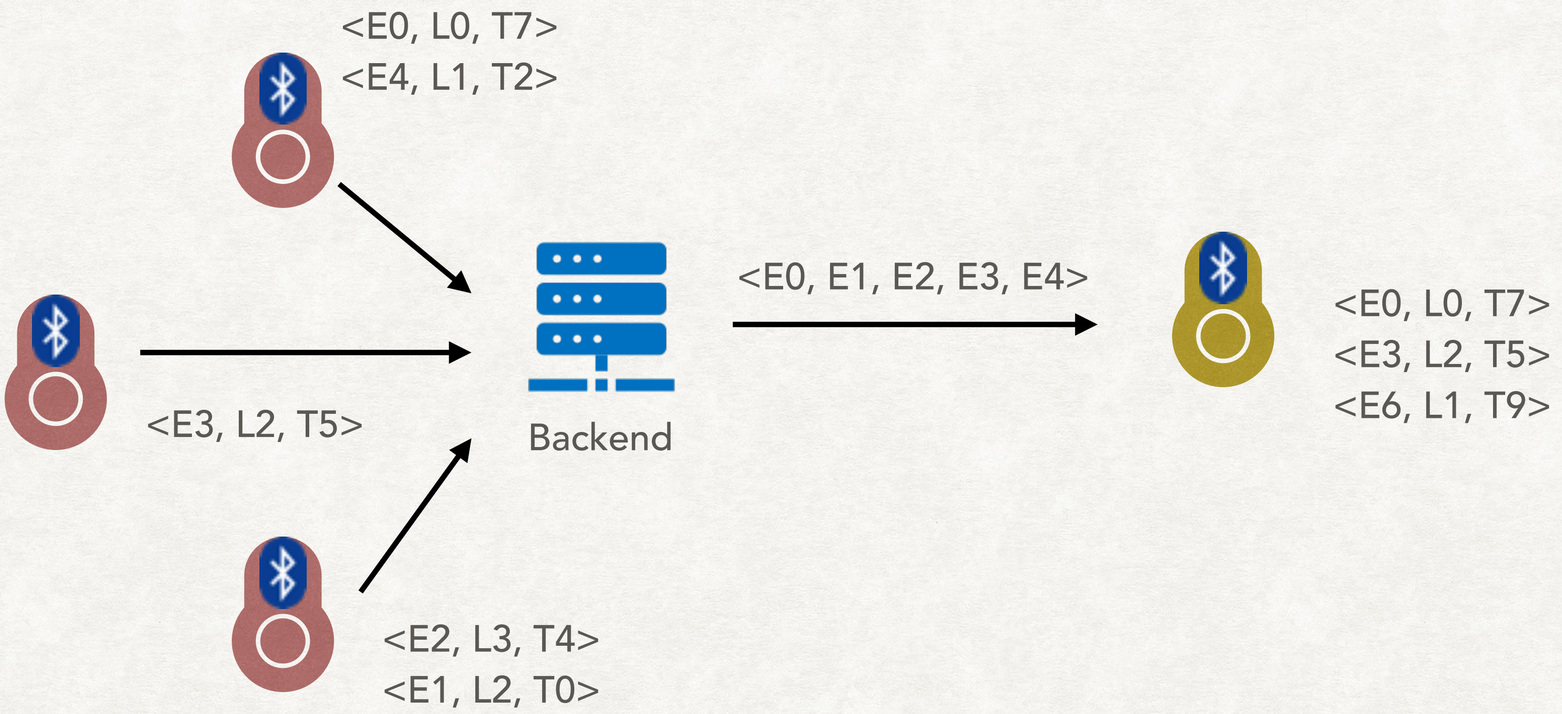
RISK DISSEMINATION

Overview



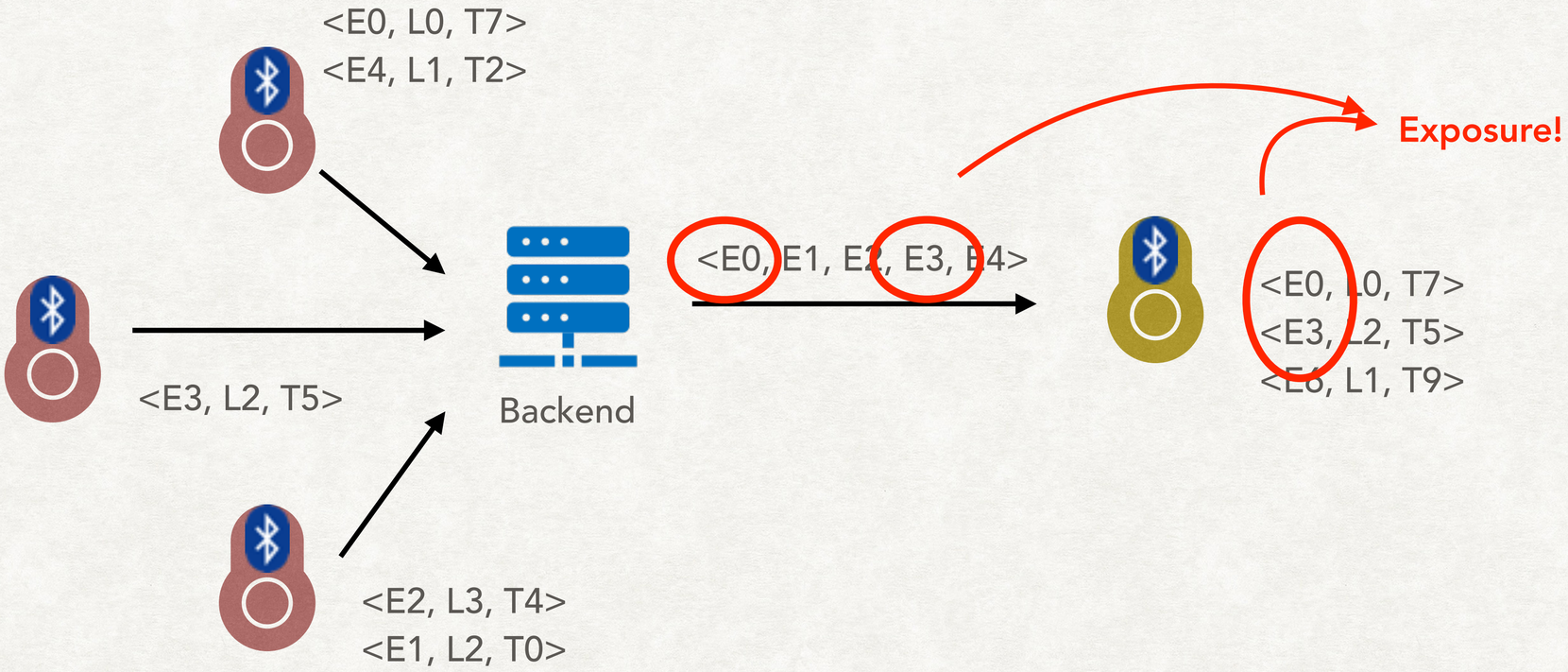
RISK DISSEMINATION

Overview



RISK DISSEMINATION

Overview



RISK DISSEMINATION

Key Requirements

- Correct information
- Preserve privacy of diagnosed individuals
- Preserve privacy of users seeking risk information
- Timely dissemination
- Low bandwidth, power, compute cost for user devices

RISK DISSEMINATION

Key Requirements

- Correct information ➡ **Risk data signed by backend**
- Preserve privacy of diagnosed individuals
- Preserve privacy of users seeking risk information
- Timely dissemination
- Low bandwidth, power, compute cost for user devices

RISK DISSEMINATION

Key Requirements

- Correct information ➡ **Risk data signed by backend**
- Preserve privacy of diagnosed individuals ➡ **Add junk entries using differential privacy**
- Preserve privacy of users seeking risk information
- Timely dissemination
- Low bandwidth, power, compute cost for user devices

RISK DISSEMINATION

Key Requirements

- Correct information ➡ **Risk data signed by backend**
- Preserve privacy of diagnosed individuals ➡ **Add junk entries using differential privacy**
- Preserve privacy of users seeking risk information ➡ **Ideally, using broadcast**
  ➡ **But this is inefficient …**
- Timely dissemination
- Low bandwidth, power, compute cost for user devices

RISK DISSEMINATION ESTIMATES

RISK DISSEMINATION ESTIMATES

$$\text{risk-data/day} = \underbrace{(\#new\text{-}cases/day * max\text{-}enctrs/day}_{\#risk\text{-}entries/day} + \Delta) * sizeof(ephID) \text{ bytes}$$

RISK DISSEMINATION ESTIMATES

$$\text{risk-data/day} = \underbrace{(\#new\text{-}cases/day * max\text{-}enctrs/day + \Delta)}_{\#risk\text{-}entries/day} * sizeof(ephID) \text{ bytes}$$

Assume new encounter every
5 min throughout the day
➡ 4032 encounters in 14 days

RISK DISSEMINATION ESTIMATES

$$\text{risk-data/day} = \underbrace{(\#\textit{new-cases/day} * \textit{max-enctrs/day}}_{\#\textit{risk-entries/day}} + \Delta) * \textit{sizeof}(\textit{ephID}) \text{ bytes}$$

Assume new encounter every 5 min throughout the day
➡ 4032 encounters in 14 days

DP noise: ~300K entries at 99th percentile

RISK DISSEMINATION ESTIMATES

$$\text{risk-data/day} = \underbrace{(\#new\text{-}cases/day * max\text{-}enctrs/day}_{\#risk\text{-}entries/day} + \Delta) * sizeof(ephID) \text{ bytes}$$

Assume new encounter every 5 min throughout the day
➡ 4032 encounters in 14 days

DP noise: ~300K entries at 99th percentile

With cuckoo filter, compress from 15 bytes to 27 bits with 0.01% false positive rate

RISK DISSEMINATION ESTIMATES

$$\text{risk-data/day} = \underbrace{(\#\textit{new-cases/day} * \textit{max-enctrs/day}}_{\#\textit{risk-entries/day}} + \Delta) * \textit{sizeof}(\textit{ephID}) \text{ bytes}$$

Assume new encounter every 5 min throughout the day
➡ 4032 encounters in 14 days

DP noise: ~300K entries at 99th percentile

With cuckoo filter, compress from 15 bytes to 27 bits with 0.01% false positive rate

Country	# new cases/day	# risk entries/day	Bytes/day (MiB)
Australia	18	390,838	1.258
Germany	3346	13,809,334	44.447
Italy	3821	15,724,534	50.612
France	16036	64,975,414	209.133
Brazil	26429	106,879,990	344.009
USA	48639	196,430,710	632.242
India	72019	290,698,870	935.658

https://www.worldometers.info/coronavirus/ (based on Oct 2020)

RISK DISSEMINATION ESTIMATES

$$\text{risk-data/day} = \underbrace{(\#\textit{new-cases/day} * \textit{max-enctrs/day}}_{\#\textit{risk-entries/day}} + \Delta) * \textit{sizeof}(\textit{ephID}) \text{ bytes}$$

Assume new encounter every 5 min throughout the day
➡ 4032 encounters in 14 days

DP noise: ~300K entries at 99th percentile

With cuckoo filter, compress from 15 bytes to 27 bits with 0.01% false positive rate

Country	# new cases/day	# risk entries/day	Bytes/day (MiB)	Delay (s)
Australia	18	390,838	1.258	13.191
Germany	3346	13,809,334	44.447	466.065
Italy	3821	15,724,534	50.612	530.703
France	16036	64,975,414	209.133	2192.92
Brazil	26429	106,879,990	344.009	3607.2
USA	48639	196,430,710	632.242	6629.54
India	72019	290,698,870	935.658	9811.09

Assuming BLE xput of ~0.8 Mbps

https://www.worldometers.info/coronavirus/ (based on Oct 2020)

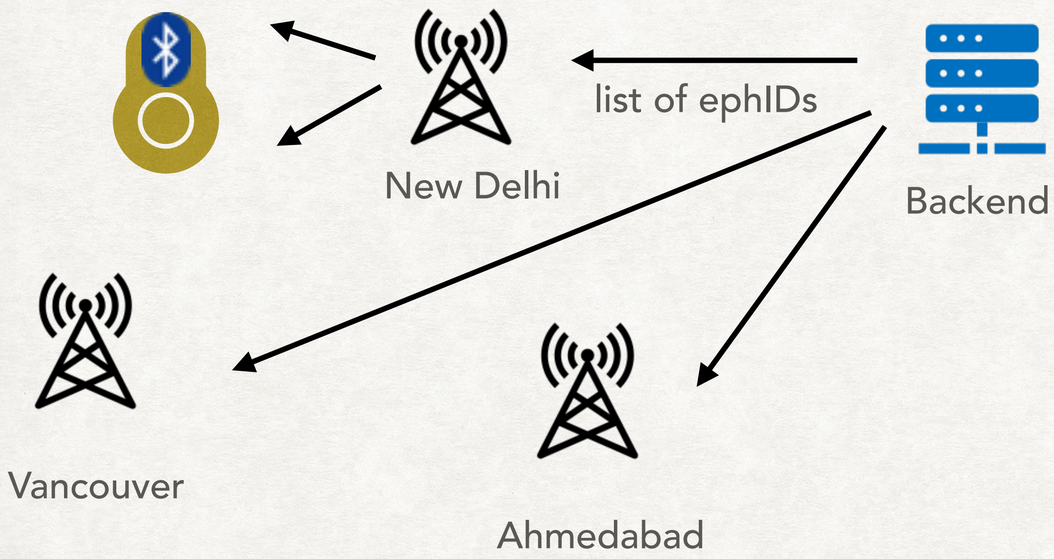
DISSEMINATION PROTOCOL

DISSEMINATION PROTOCOL

Broadcast protocol

Network beacons broadcast risk data of local region

Dongles **passively listen** to a network beacon

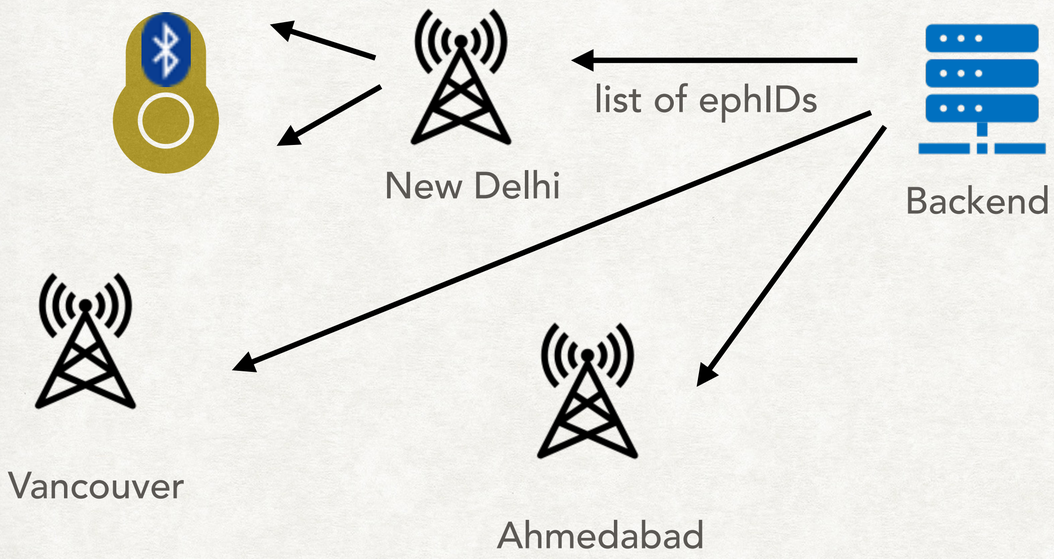


DISSEMINATION PROTOCOL

Broadcast protocol

Network beacons broadcast risk data of local region

Dongles **passively listen** to a network beacon



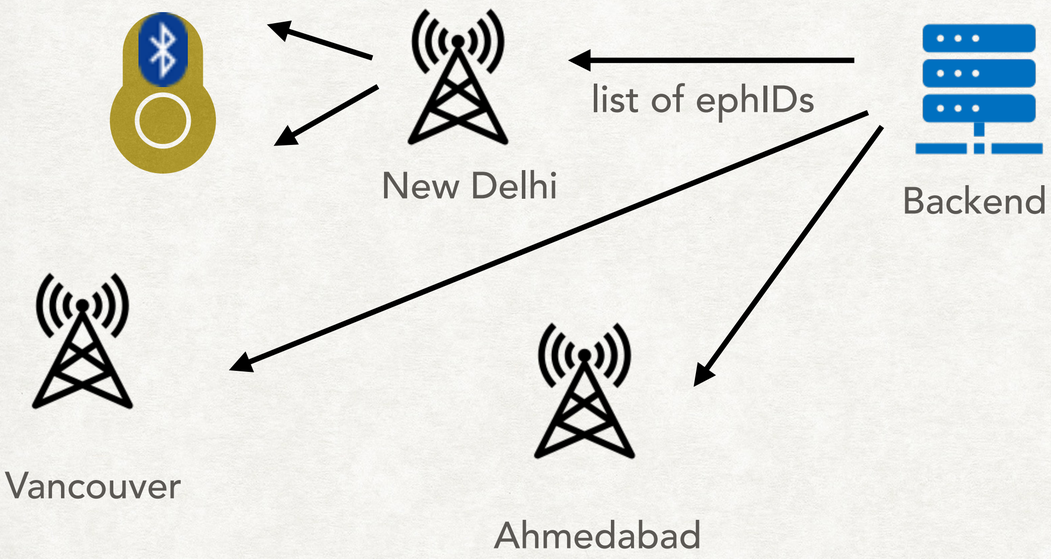
Problem: Travellers may not get all risk information

DISSEMINATION PROTOCOL

Broadcast protocol

Network beacons broadcast risk data of local region

Dongles **passively listen** to a network beacon



Problem: Travellers may not get all risk information

Querying protocol

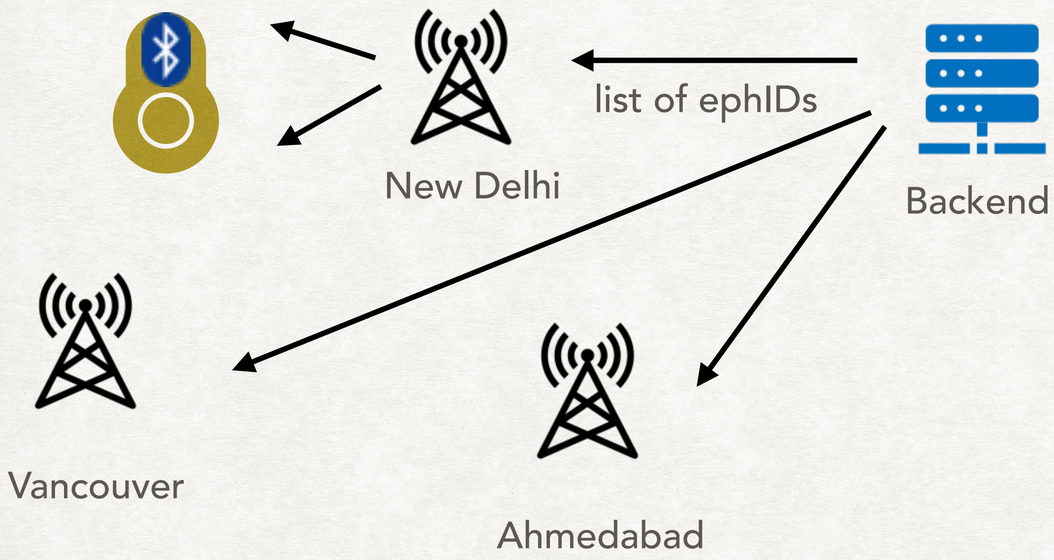
Dongles query for risk data of non-local regions

DISSEMINATION PROTOCOL

Broadcast protocol

Network beacons broadcast risk data of local region

Dongles **passively listen** to a network beacon



Problem: Travellers may not get all risk information

Querying protocol

Dongles query for risk data of non-local regions

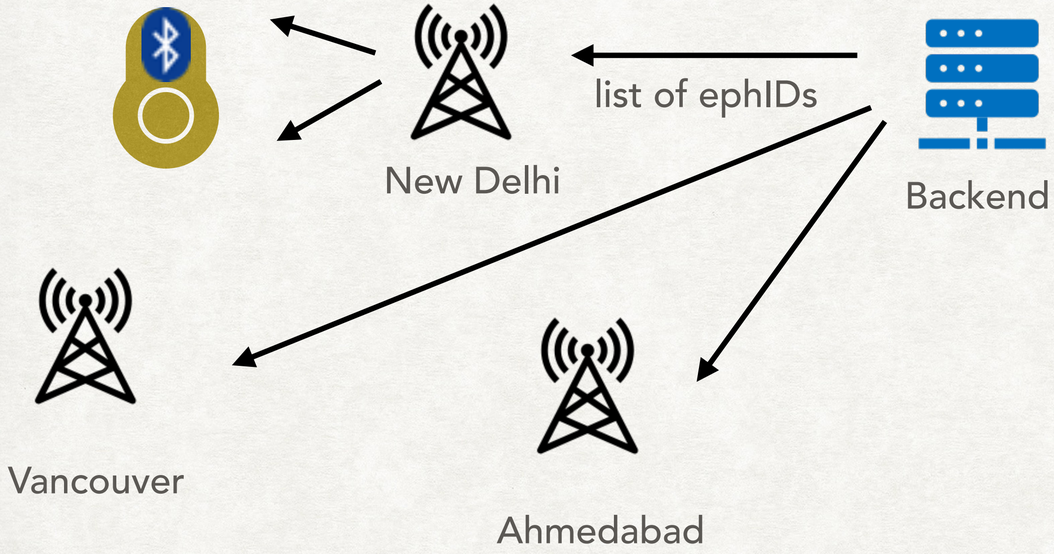
Privacy goal: hide queries and responses from backend, network beacon, eavesdroppers

DISSEMINATION PROTOCOL

Broadcast protocol

Network beacons broadcast risk data of local region

Dongles **passively listen** to a network beacon

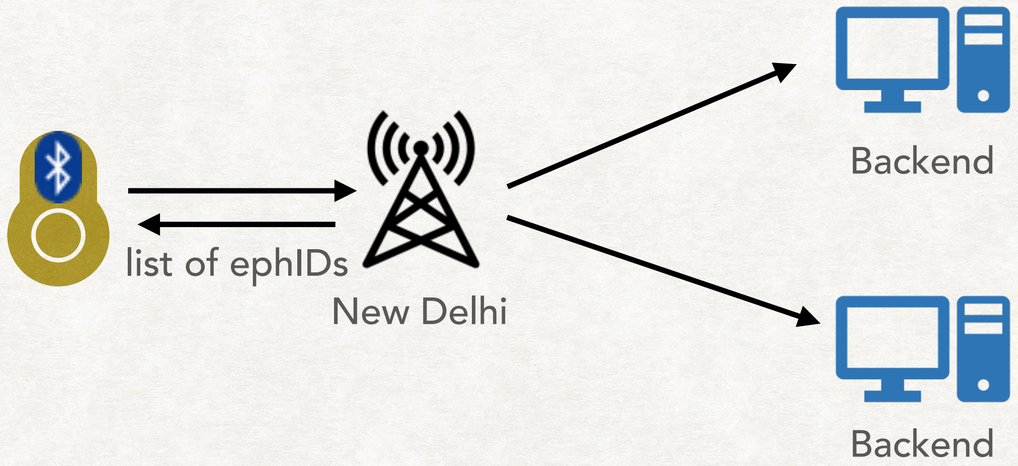


Problem: Travellers may not get all risk information

Querying protocol

Dongles query for risk data of non-local regions

Privacy goal: hide queries and responses from backend, network beacon, eavesdroppers



Our solution:

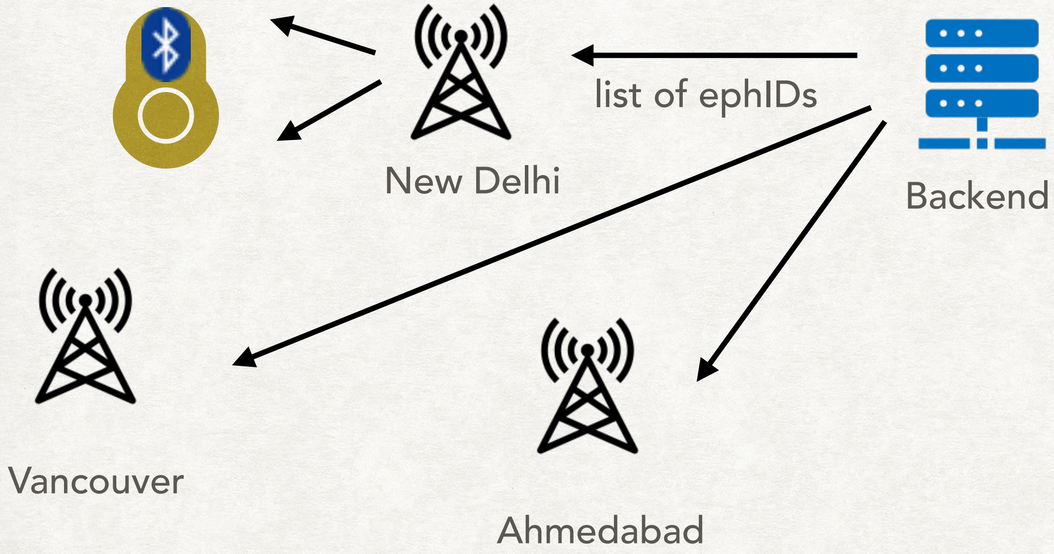
- 2-server IT-PIR protocol (information-theoretic private information retrieval) at the backend

DISSEMINATION PROTOCOL

Broadcast protocol

Network beacons broadcast risk data of local region

Dongles **passively listen** to a network beacon

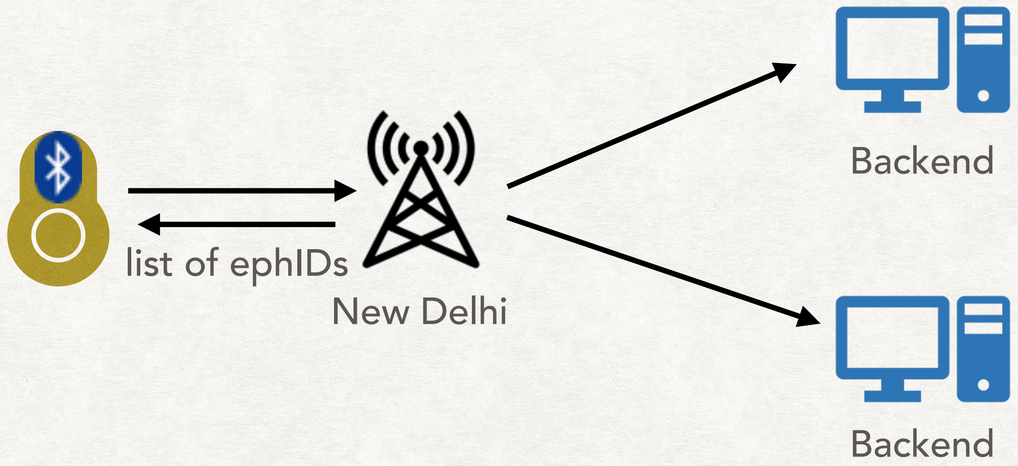


Problem: Travellers may not get all risk information

Querying protocol

Dongles query for risk data of non-local regions

Privacy goal: hide queries and responses from backend, network beacon, eavesdroppers



Our solution:

- 2-server IT-PIR protocol (information-theoretic private information retrieval) at the backend
- End-to-end encryption between dongle, backend

2-SERVER IT-PIR PROTOCOL

Assumption: non-colluding servers

- e.g., using two different cloud providers or heterogeneous hardware TEEs

Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private Information Retrieval. Foundations of Computer Science, 1995

2-SERVER IT-PIR PROTOCOL

Assumption: non-colluding servers

- e.g., using two different cloud providers or heterogeneous hardware TEEs

$$D = < B[i] >$$

Server S1

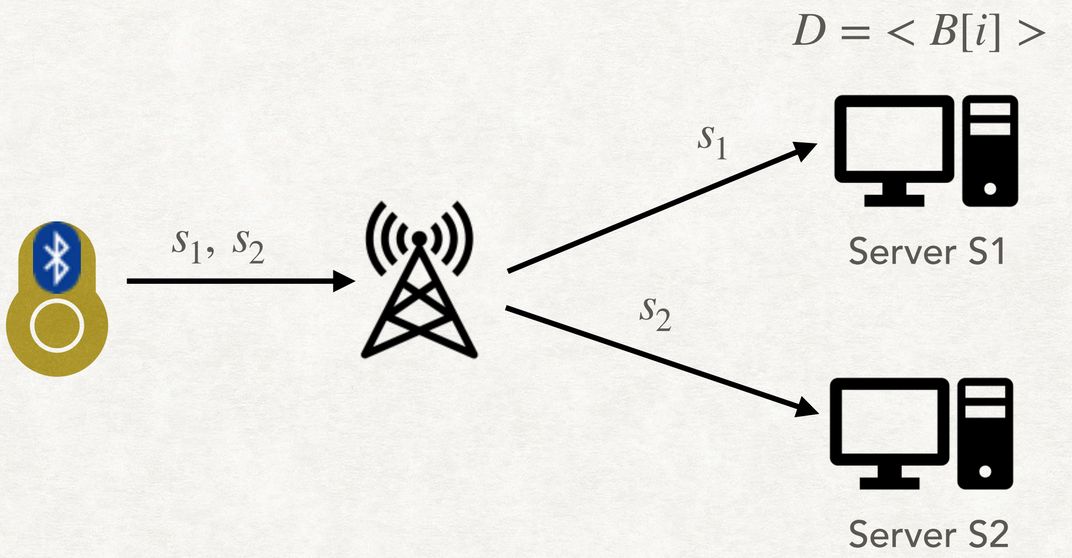
Server S2

Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private Information Retrieval. Foundations of Computer Science, 1995

2-SERVER IT-PIR PROTOCOL

Assumption: non-colluding servers

- e.g., using two different cloud providers or heterogeneous hardware TEEs



s_1	0	0	1	0
s_2	0	1	1	0

D	B[0]	B[1]	B[2]	B[3]

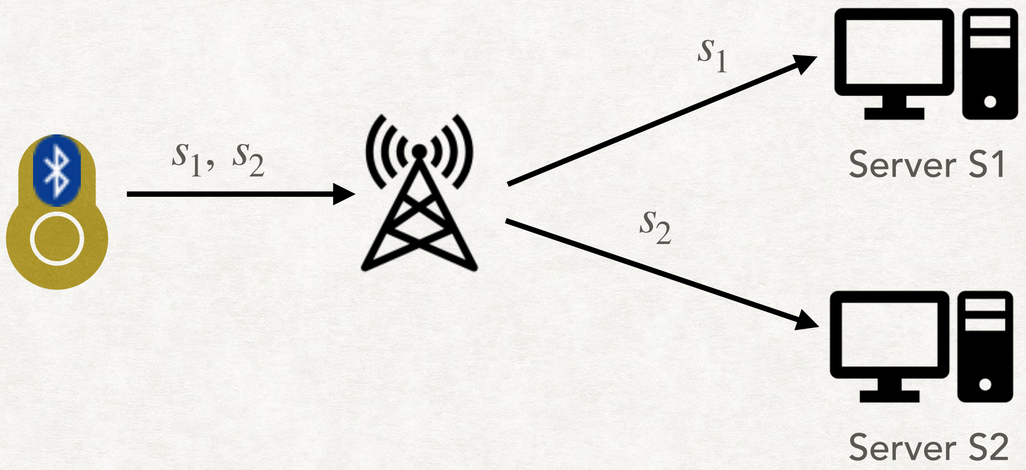
Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private Information Retrieval. Foundations of Computer Science, 1995

2-SERVER IT-PIR PROTOCOL

Assumption: non-colluding servers

- e.g., using two different cloud providers or heterogeneous hardware TEEs

$D = < B[i] >$



$$B_1 = \bigoplus_{i=0}^{N} s_1[i] \,.\, B[i]$$

$$B_2 = \bigoplus_{i=0}^{N} s_2[i] \,.\, B[i]$$

s_1 | 0 | 0 | 1 | 0 |

s_2 | 0 | 1 | 1 | 0 |

D | B[0] | B[1] | B[2] | B[3] |

$B_1 = B[2]$

$B_2 = B[1] \oplus B[2]$

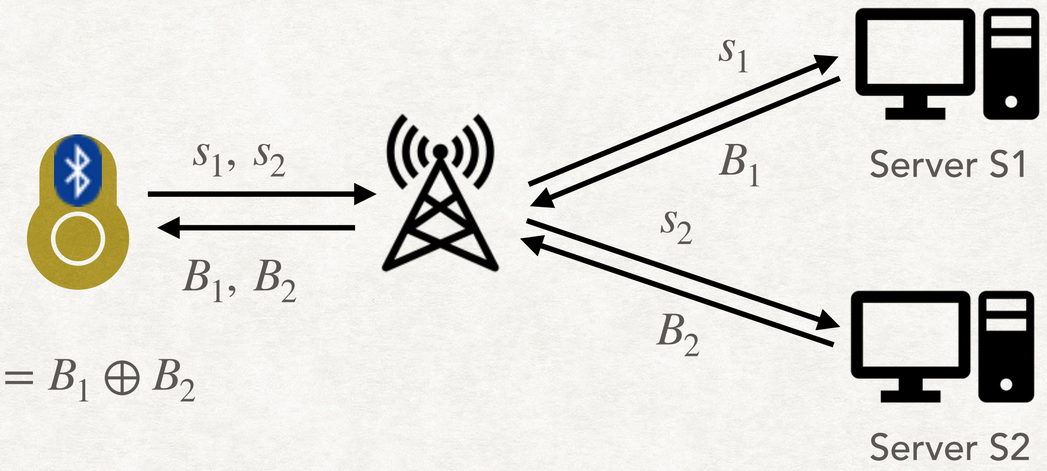
Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private Information Retrieval. Foundations of Computer Science, 1995

2-SERVER IT-PIR PROTOCOL

Assumption: non-colluding servers

- e.g., using two different cloud providers or heterogeneous hardware TEEs

$D = < B[i] >$



$B = B_1 \oplus B_2$

$$B_1 = \bigoplus_{i=0}^{N} s_1[i] \,.\, B[i]$$

$$B_2 = \bigoplus_{i=0}^{N} s_2[i] \,.\, B[i]$$

s_1 | 0 | 0 | 1 | 0 |

s_2 | 0 | 1 | 1 | 0 |

D | B[0] | B[1] | B[2] | B[3] |

$B_1 = B[2]$

$B_2 = B[1] \oplus B[2]$

Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private Information Retrieval. Foundations of Computer Science, 1995

PANCAST PROTOCOL

Key challenge: Infection rates may vary widely across regions and times

What is a “good” uniform block (region) size?

Small regions ➡ query bandwidth
Large regions ➡ response bandwidth

PANCAST PROTOCOL

Key challenge: Infection rates may vary widely across regions and times

What is a “good” uniform block (region) size?

Small regions ➡ query bandwidth
Large regions ➡ response bandwidth

Our solution

1. Dynamically adapt regions to maintain a uniform block size

PANCAST PROTOCOL

Key challenge: Infection rates may vary widely across regions and times

What is a "good" uniform block (region) size?

Small regions ➡ query bandwidth
Large regions ➡ response bandwidth

Our solution

1. Dynamically adapt regions to maintain a uniform block size

RiskDB

ephID	locID	time	
E0	L0	T7	B0
E4	L1	T2	
E1	L2	T0	B1
E3	L2	T5	
E2	L3	T4	B2 + padding

PANCAST PROTOCOL

Key challenge: Infection rates may vary widely across regions and times

What is a "good" uniform block (region) size?

Small regions ➡ query bandwidth
Large regions ➡ response bandwidth

Our solution

1. Dynamically adapt regions to maintain a uniform block size

RiskDB

ephID	locID	time	
E0	L0	T7	B0
E4	L1	T2	
E1	L2	T0	B1
E3	L2	T5	
E2	L3	T4	B2 + padding

L-map

L0	B0
L1	B0
L2	B1
L3	B2

PANCAST PROTOCOL

Key challenge: Infection rates may vary widely across regions and times

What is a "good" uniform block (region) size?

Small regions ➡ query bandwidth
Large regions ➡ response bandwidth

Our solution

1. Dynamically adapt regions to maintain a uniform block size

RiskDB

ephID	locID	time	
E0	L0	T7	B0
E4	L1	T2	
E1	L2	T0	B1
E3	L2	T5	
E2	L3	T4	B2 + padding

L-map

L0	B0
L1	B0
L2	B1
L3	B2

2. Dongles use two rounds of PIR

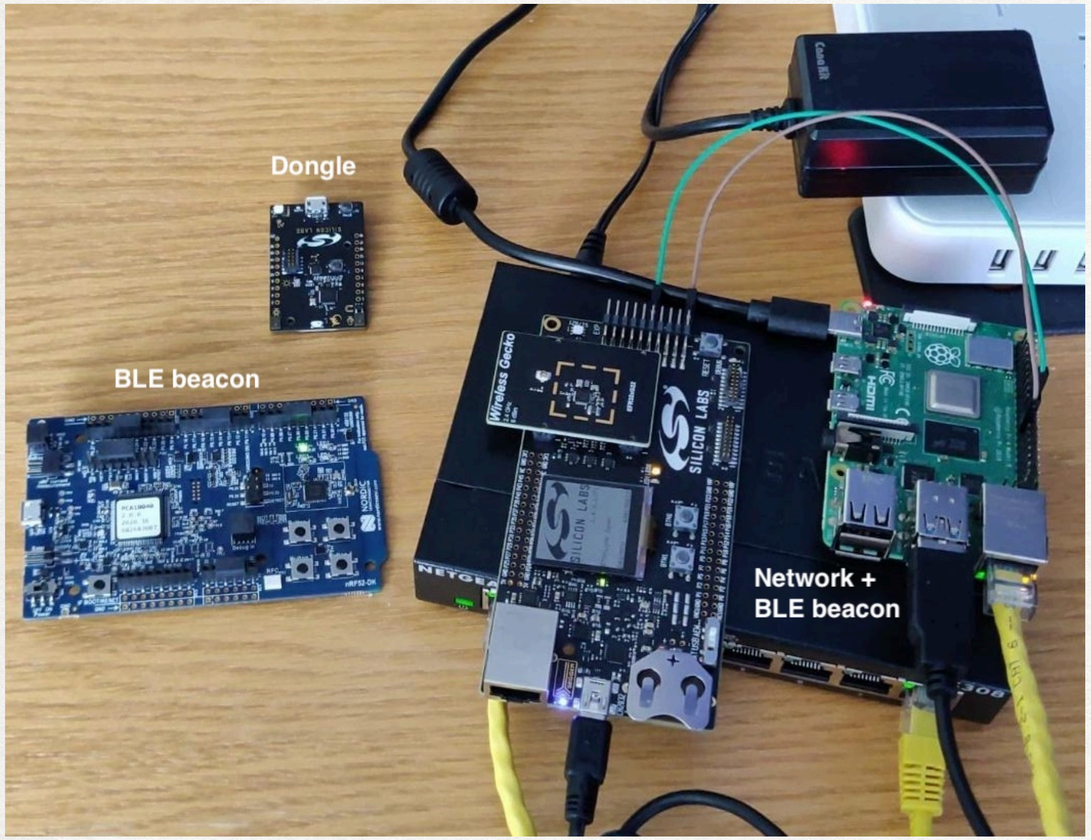
- Round 1: block idx = PIR(loc id)
- Round 2: block = PIR(block idx)

OUTLINE

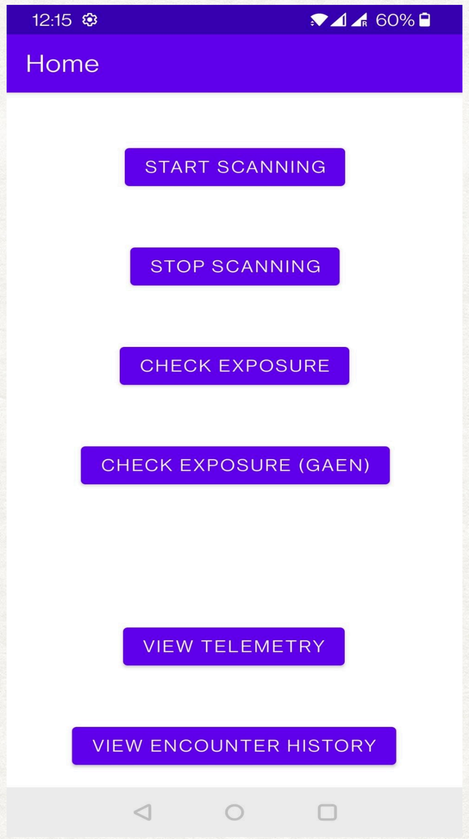
- Risk dissemination
- Implementation and evaluation
- Deployment

IMPLEMENTATION

PanCast devices



Smartphone app



Dev Kits: ~300 CAD/~18K INR

Production: ~20 CAD/~1200 INR

Network beacons can be integrated with wifi base stations

EVALUATION

EVALUATION

Risk download latency

Broadcast: BLE periodic broadcast @10 ms

Querying: BLE connection oriented comm.

EVALUATION

Risk download latency

Broadcast: BLE periodic broadcast @10 ms

Querying: BLE connection oriented comm.

Payload size: 5 MB (~1.5 million risk entries)

Operation	Latency (s)
Broadcast	315
Querying	61

EVALUATION

Risk download latency

Broadcast: BLE periodic broadcast @10 ms

Querying: BLE connection oriented comm.

Payload size: 5 MB (~1.5 million risk entries)

Operation	Latency (s)
Broadcast	315
Querying	61

Battery life

Operation	Current	Normalized current in an hour
Base current	0.10 mA	0.10 mA
BLE Scanning	3.77 mA	0.19 mA
Encounter logging	2.60 mA	0.01 mA
Crypto	2.50 mA	~10^{-4} mA

EVALUATION

Risk download latency

Broadcast: BLE periodic broadcast @10 ms

Querying: BLE connection oriented comm.

Payload size: 5 MB (~1.5 million risk entries)

Operation	Latency (s)
Broadcast	315
Querying	61

Battery life

Operation	Current	Normalized current in an hour
Base current	0.10 mA	0.10 mA
BLE Scanning	3.77 mA	0.19 mA
Encounter logging	2.60 mA	0.01 mA
Crypto	2.50 mA	~10^{-4} mA

Typical coin cells: 220 mAh

Expected battery life: $\frac{220}{0.1 + 0.19 + 0.01} \approx 33$ days

INCREMENTAL DEPLOYMENT AND INTEROPERABILITY

Strategic deployment of beacons

- e.g. prioritize restaurants, supermarkets, schools over forests

INCREMENTAL DEPLOYMENT AND INTEROPERABILITY

Strategic deployment of beacons

- e.g. prioritize restaurants, supermarkets, schools over forests

Interoperate with manual tracing

- Provides utility even with low user adoption

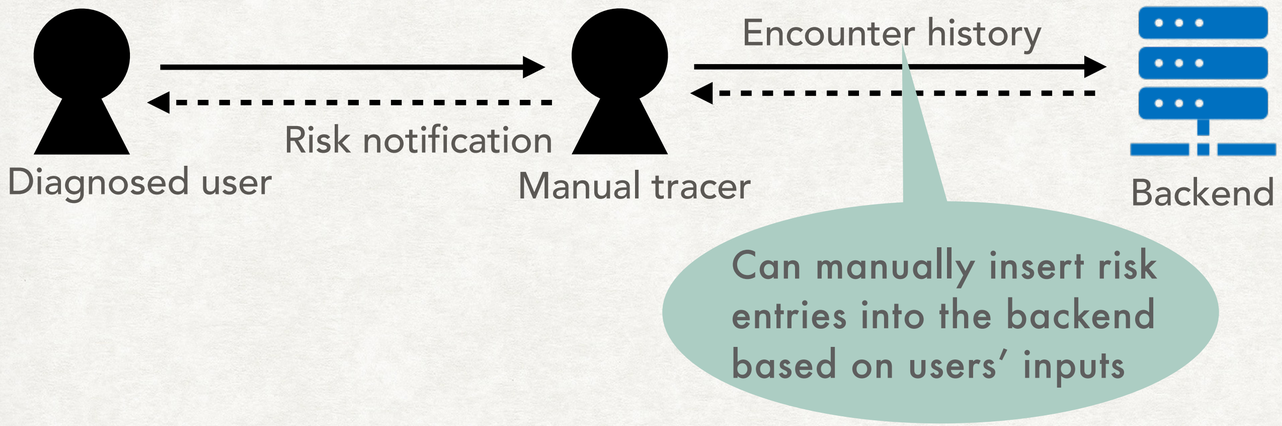
INCREMENTAL DEPLOYMENT AND INTEROPERABILITY

Strategic deployment of beacons

- e.g. prioritize restaurants, supermarkets, schools over forests

Interoperate with manual tracing

- Provides utility even with low user adoption



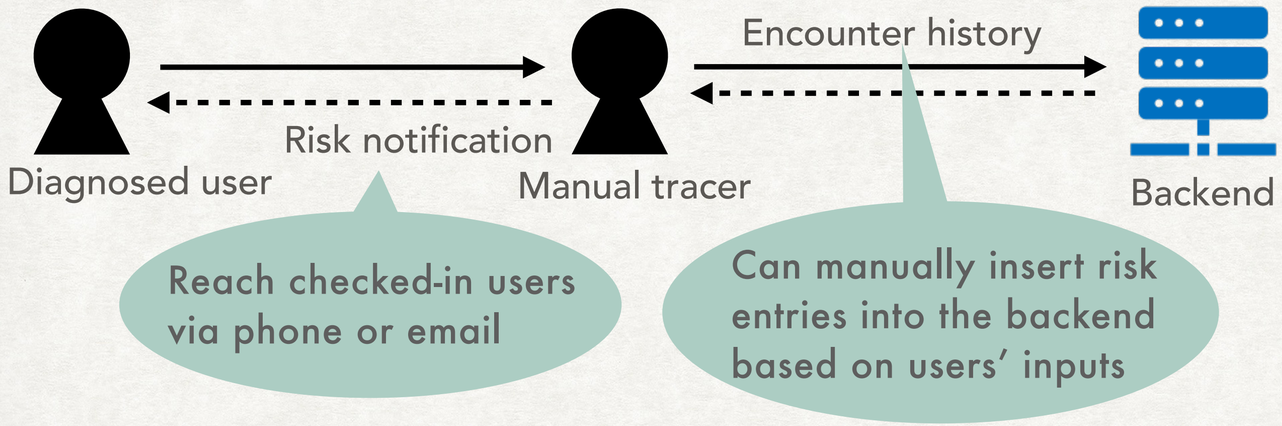
INCREMENTAL DEPLOYMENT AND INTEROPERABILITY

Strategic deployment of beacons

- e.g. prioritize restaurants, supermarkets, schools over forests

Interoperate with manual tracing

- Provides utility even with low user adoption



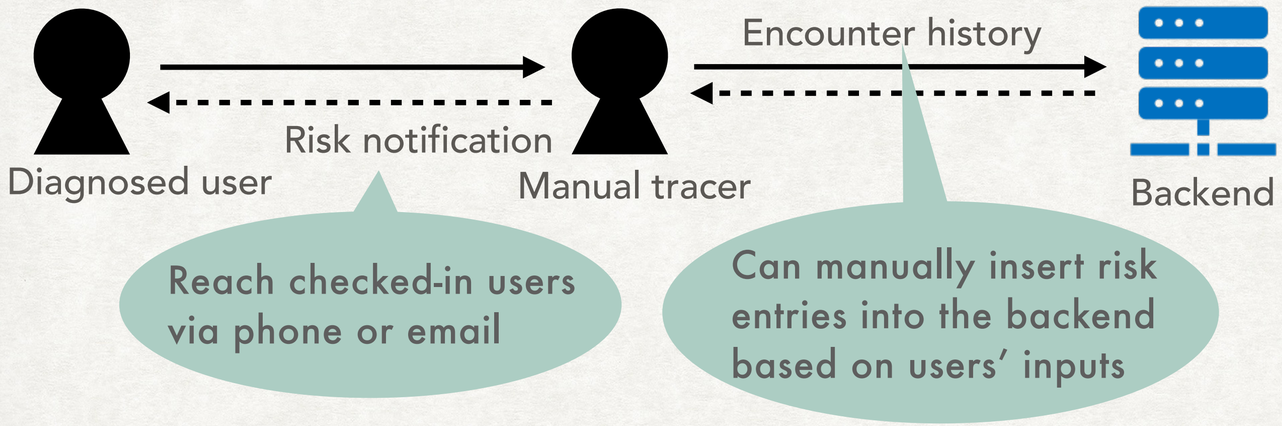
INCREMENTAL DEPLOYMENT AND INTEROPERABILITY

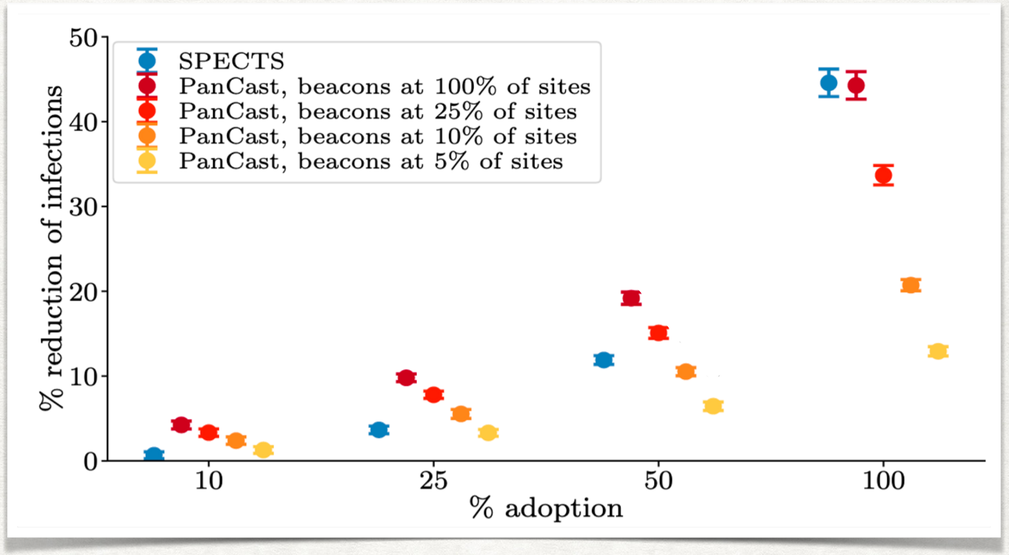
Strategic deployment of beacons

- e.g. prioritize restaurants, supermarkets, schools over forests

Interoperate with manual tracing

- Provides utility even with low user adoption





More simulation results in Scientific Reports 2022:
https://www.nature.com/articles/s41598-022-09440-1.pdf

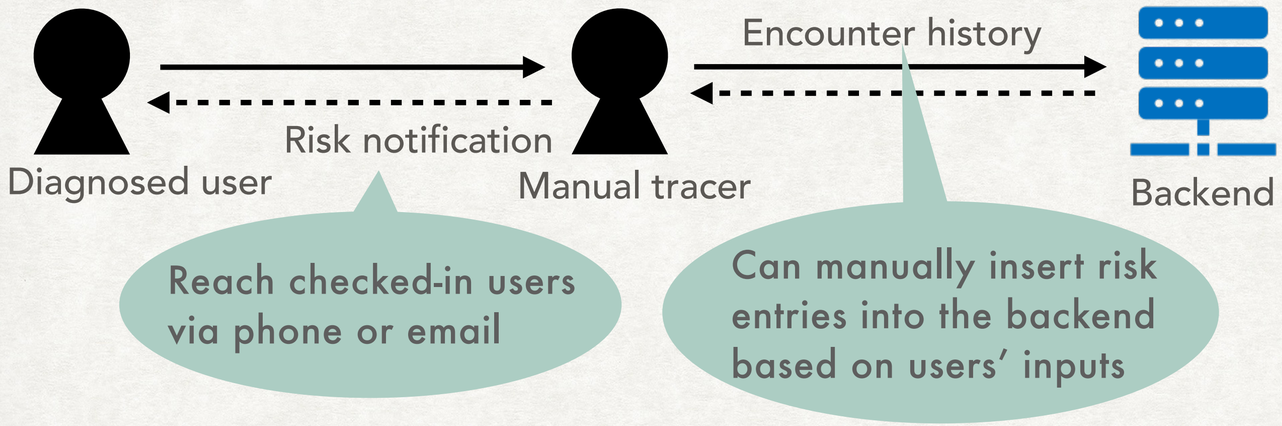
INCREMENTAL DEPLOYMENT AND INTEROPERABILITY

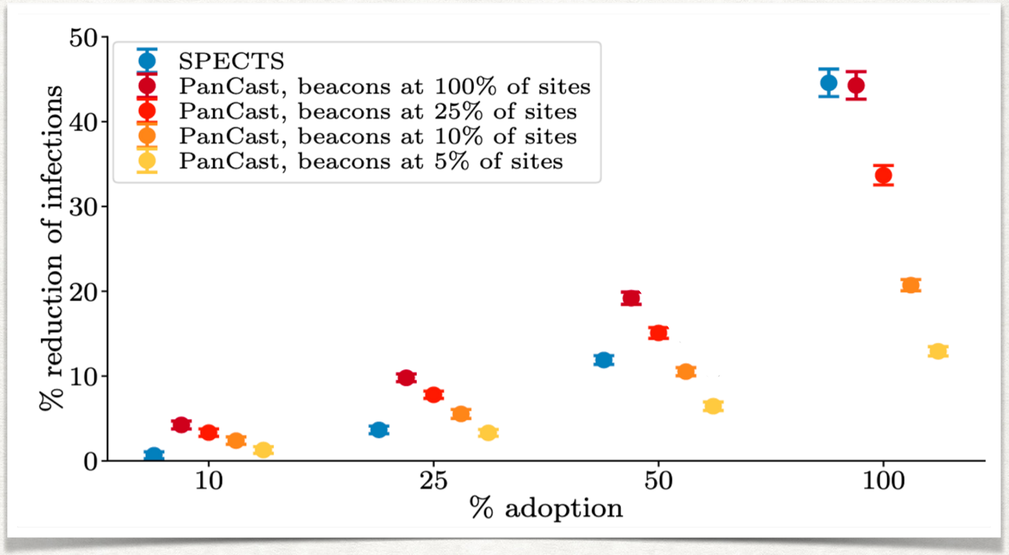
Strategic deployment of beacons

- e.g. prioritize restaurants, supermarkets, schools over forests

Interoperate with manual tracing

- Provides utility even with low user adoption





More simulation results in Scientific Reports 2022:
https://www.nature.com/articles/s41598-022-09440-1.pdf

Complement existing SPECTs

- Broadcast GAEN-compatible ephIDs from beacons to users' phone apps

ONGOING WORK

Deployment

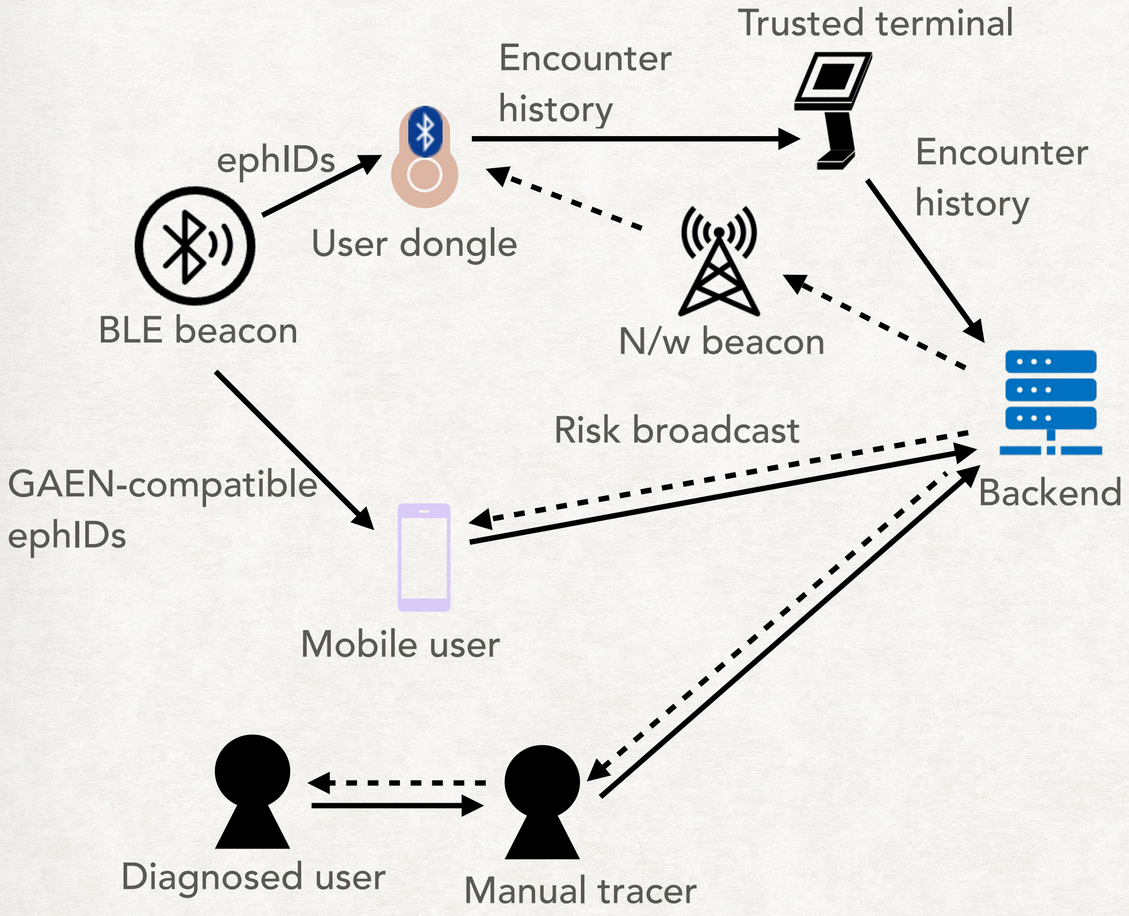
- Ran a pilot deployment with simulated infection transmissions @ UBC CS
- Future: Perform a real-world deployment
- Dataset generation
- Refining risk estimation models

Practical considerations

- Beacon placement density
- Handling clock synchronizations
- Visualization support for dongle data via users' personal devices

PANCAST

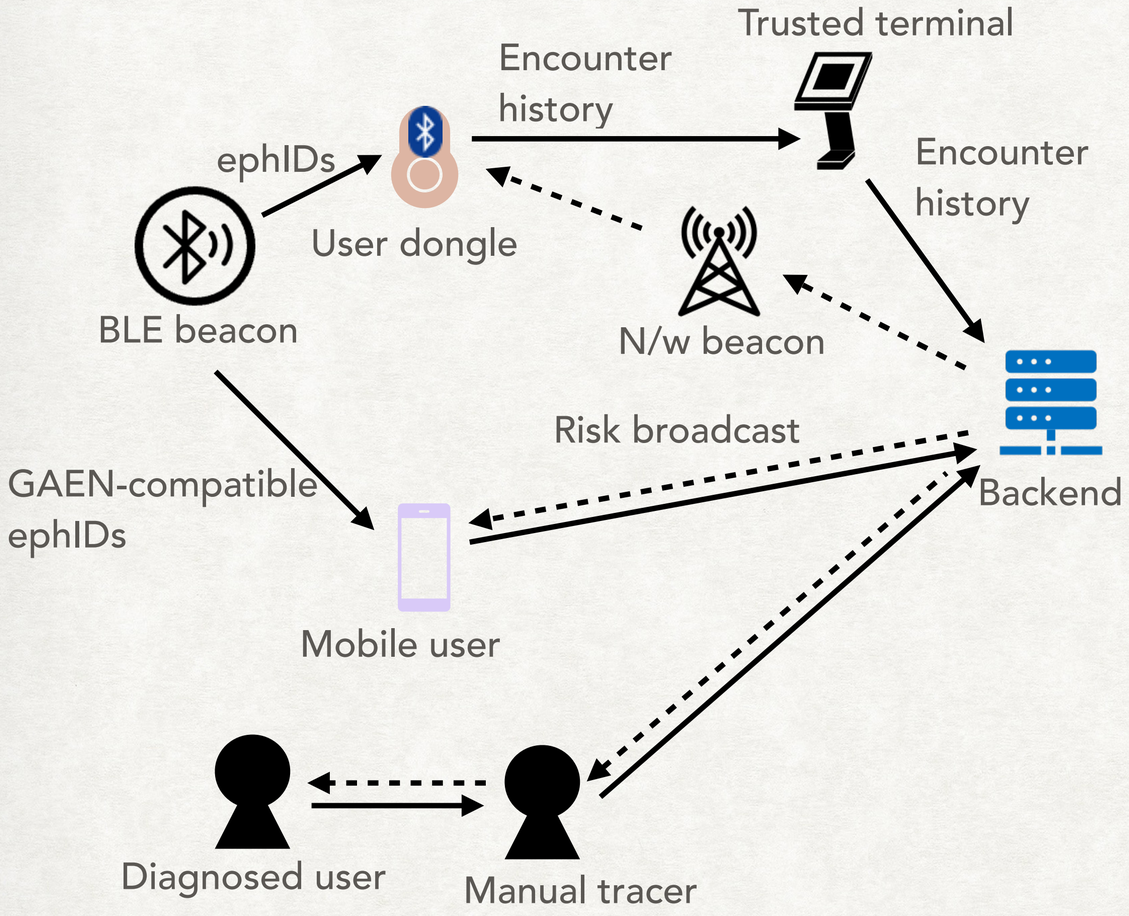
www.pancast.mpi-sws.org



Property	PanCast
Utility	• Strategically-placed beacons provide contextual info, allowing more accurate risk estimates • Useful even under partial deployment
Privacy	• Beacons only broadcast; user devices mostly passive • Decentralized risk notification • Differential privacy for patients, IT-PIR for queriers
Inclusiveness	Simple, zero-maintenance dongles, or smartphones
Interoperability	Interoperates with manual tracing; complements SPECTS

PANCAST

www.pancast.mpi-sws.org



Property	PanCast
Utility	• Strategically-placed beacons provide contextual info, allowing more accurate risk estimates • Useful even under partial deployment
Privacy	• Beacons only broadcast; user devices mostly passive • Decentralized risk notification • Differential privacy for patients, IT-PIR for queriers
Inclusiveness	Simple, zero-maintenance dongles, or smartphones
Interoperability	Interoperates with manual tracing; complements SPECTS

QUESTIONS?

BACKUP

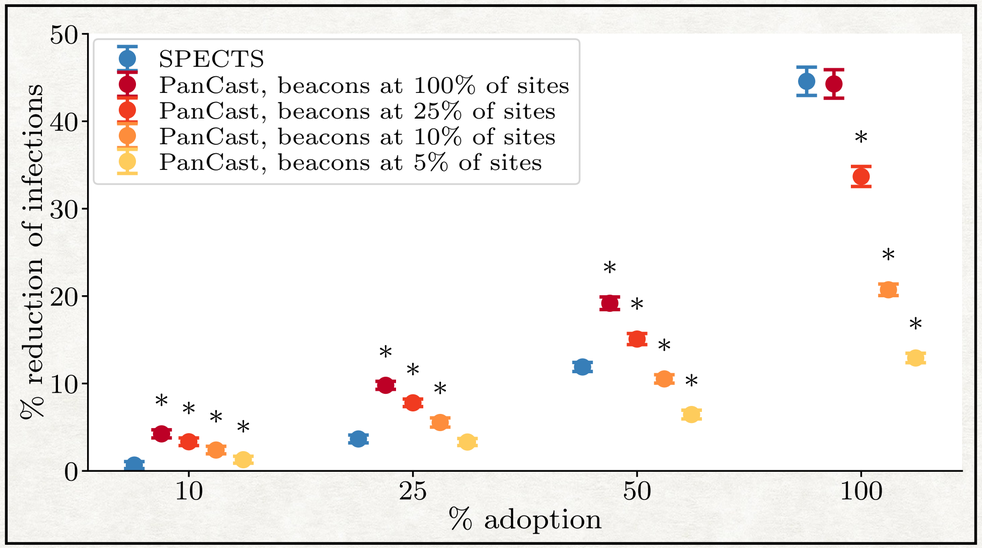
PRIVACY

Operation stage	**Backend**	**Other users**	**Network beacon**	**Terminal**
Registration	PII (e.g., phone #), user-dongle mapping, beacon-location map, devices' secret keys,	none	none	none
Encounter logging	none	none	none	none
Encounter upload	location history	none	none	upload size, location history*
Risk notification	none	common subset of location history, but anonymized**	noised broadcast size*** and time	none

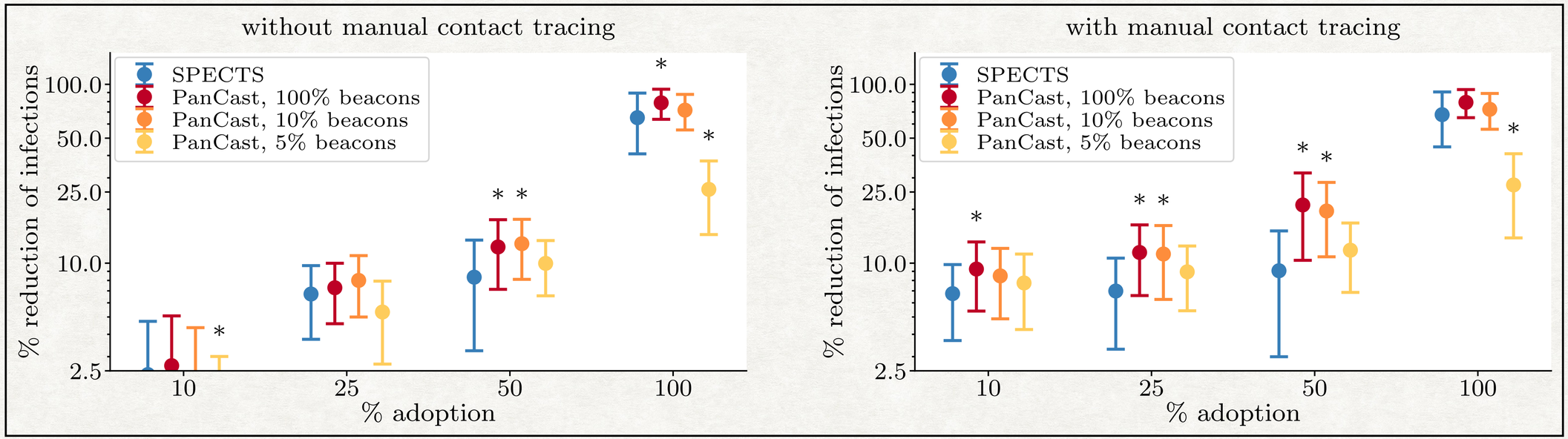
** Only if user wishes to use the terminal to select data prior to upload*

*** Other users only learn ephids of beacons where they intersected with at least one sick user*

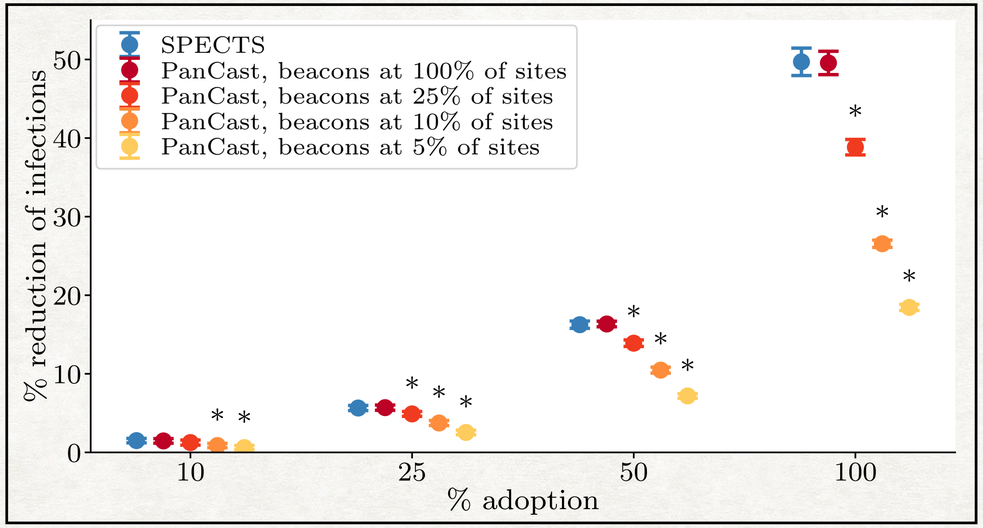
**** Beacons only observe differentially-private (noised) broadcast size (recall: Δ)*



No environmental factors; PanCast with manual tracing, SPECTS do not interoperate with manual tracing

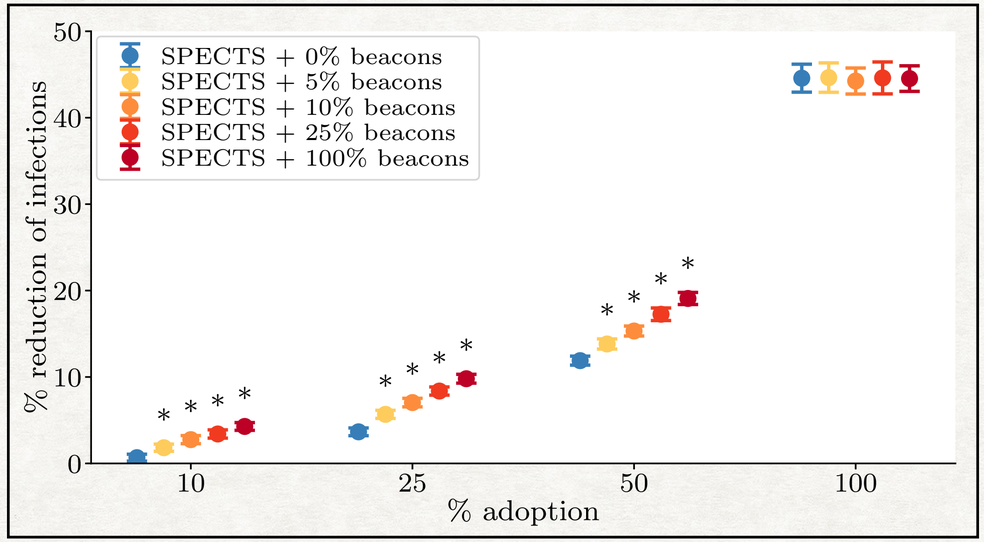


Site-dependent transmission rates in PanCast, but not SPECTS.



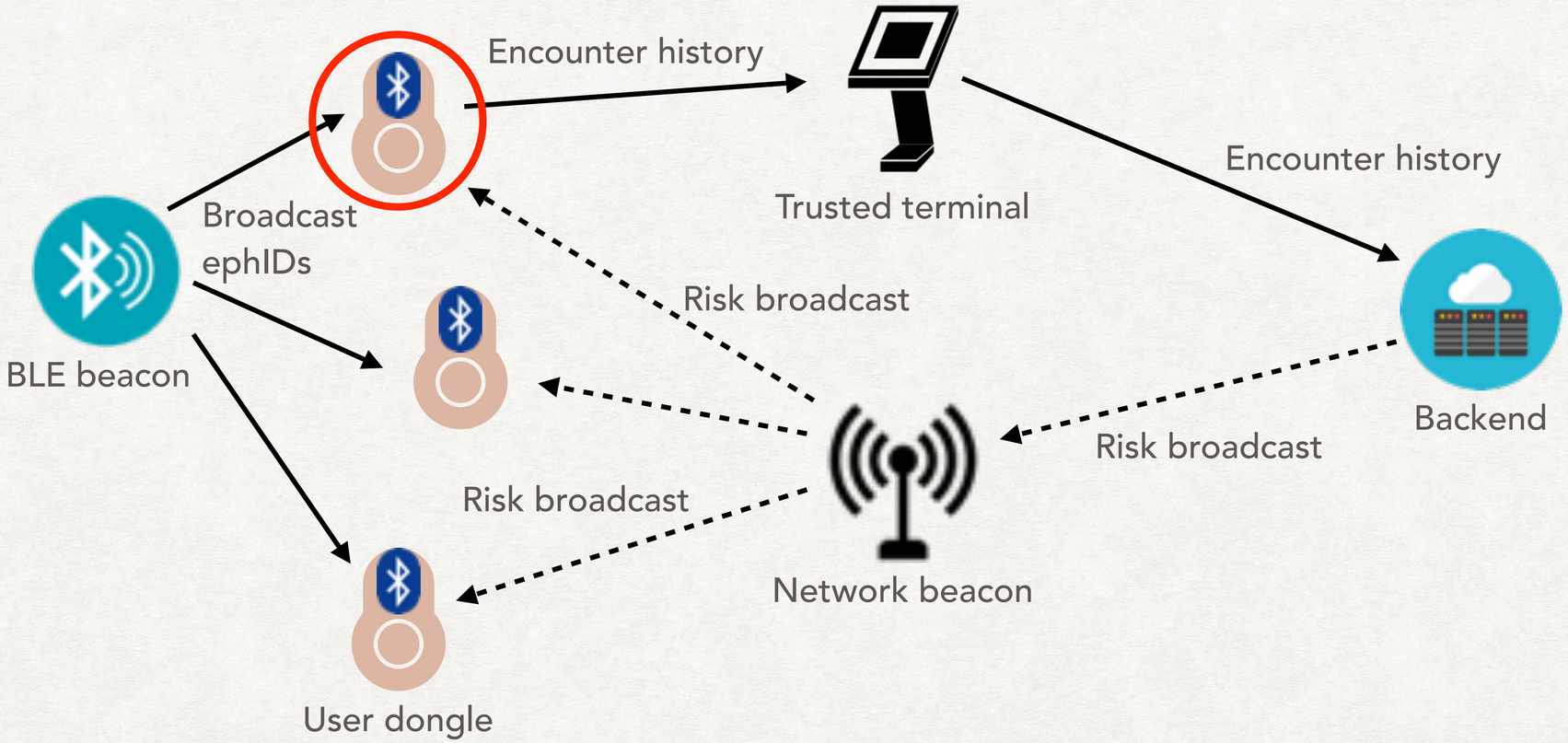
PanCast vs. SPECTS without manual tracing and without leveraging environmental factors.

PanCast performs worse than SPECTS because it is deprived of beacons, manual tracing, and environmental information

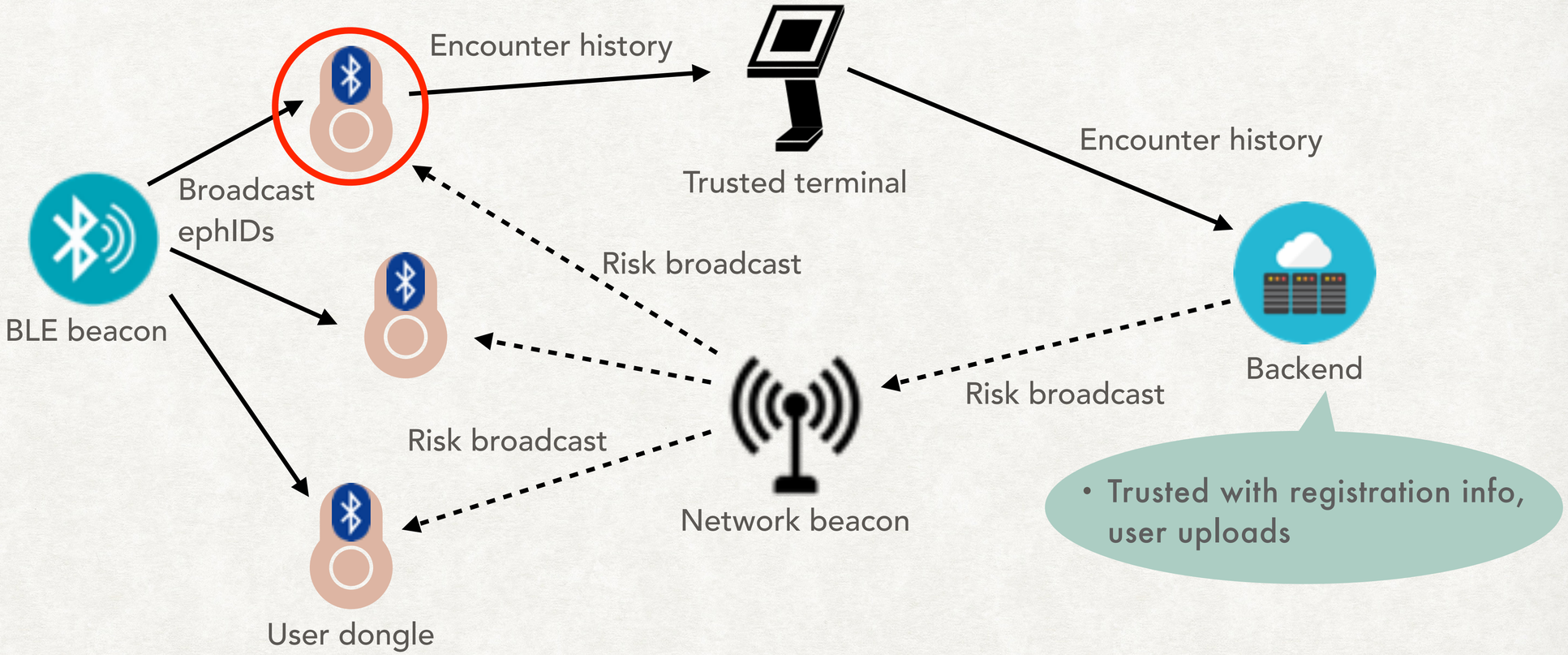


Reduction of infections with combined SPECTS + PanCast + manual tracing, but without environmental factors

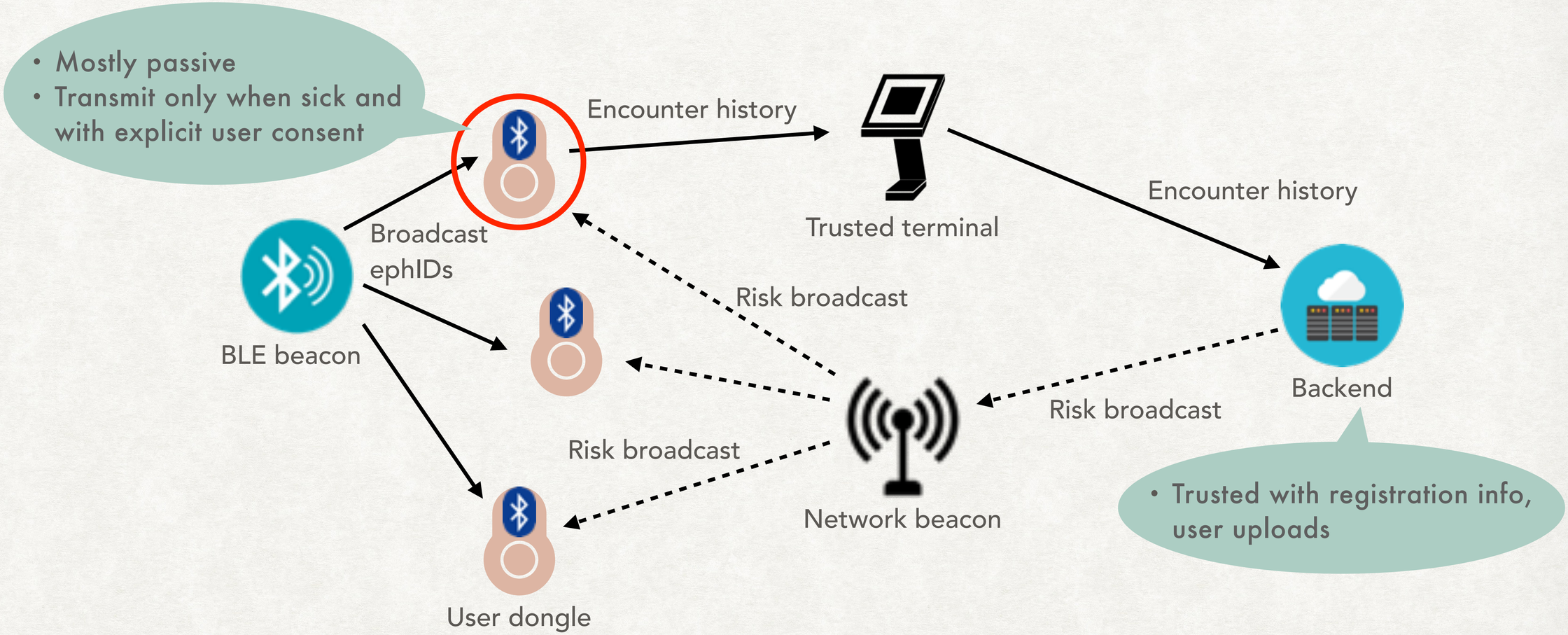
PANCAST SECURITY AND PRIVACY



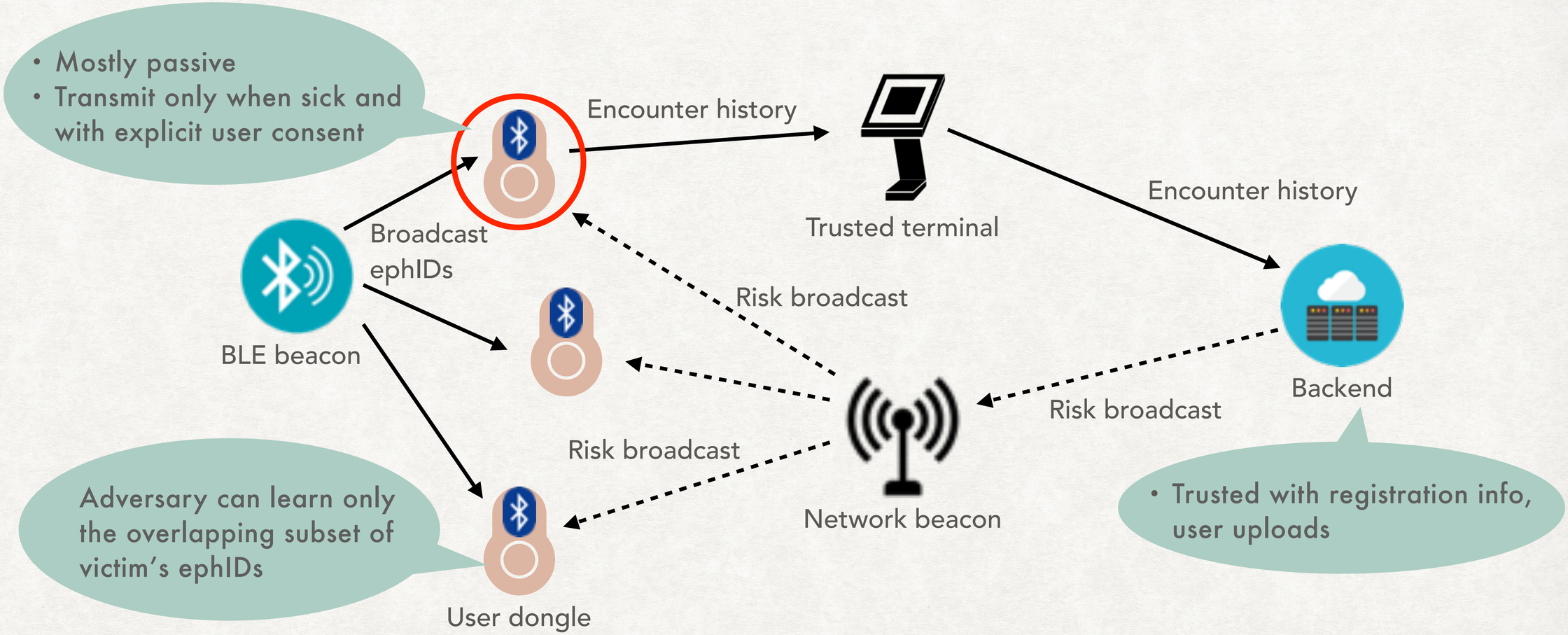
PANCAST SECURITY AND PRIVACY



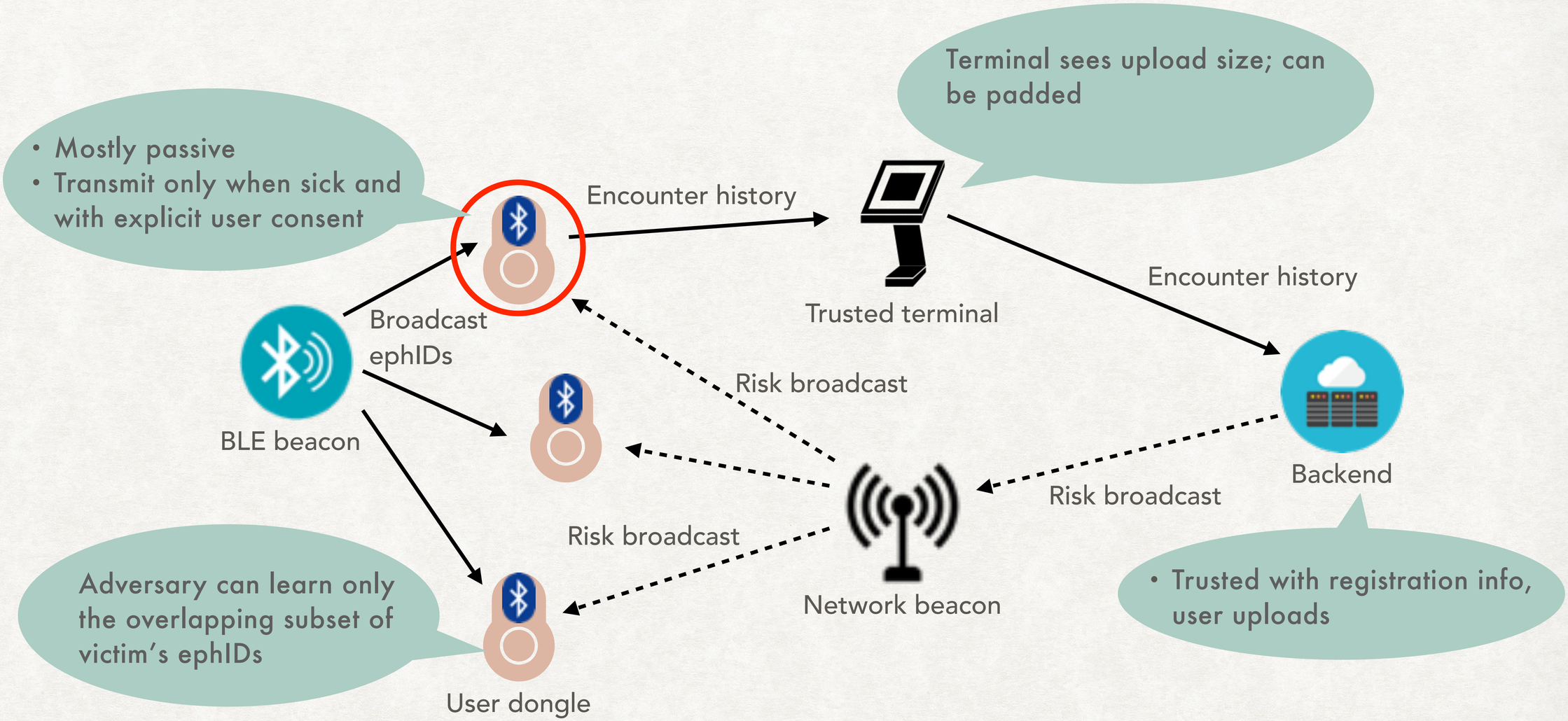
PANCAST SECURITY AND PRIVACY



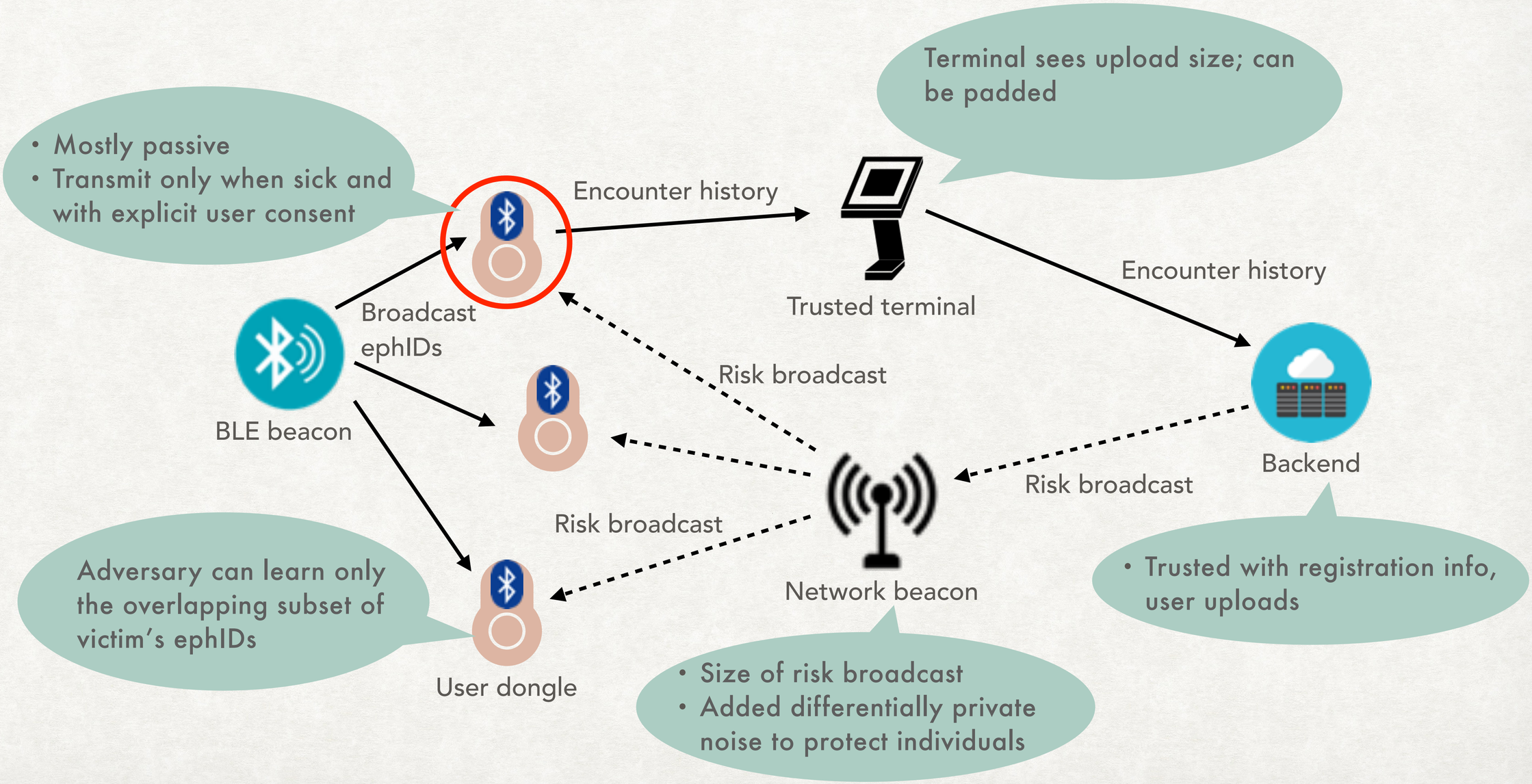
PANCAST SECURITY AND PRIVACY



PANCAST SECURITY AND PRIVACY



PANCAST SECURITY AND PRIVACY



SECURITY

- Clock inconsistencies due to beacon and dongle power failures
- Beacon location misconfiguration
- Relay attacks

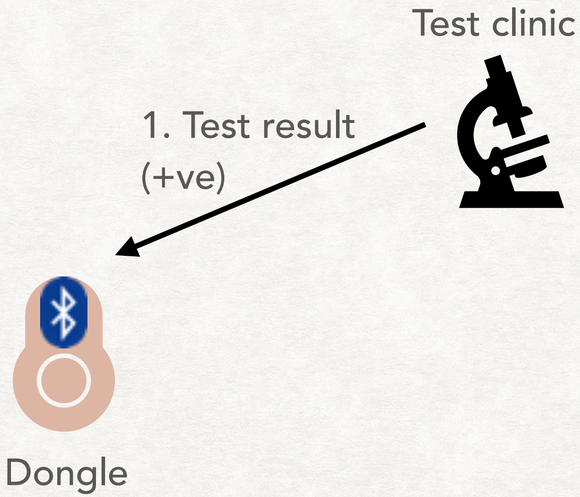
ENCOUNTER UPLOAD

ENCOUNTER UPLOAD

1. Delayed release (using personal device)

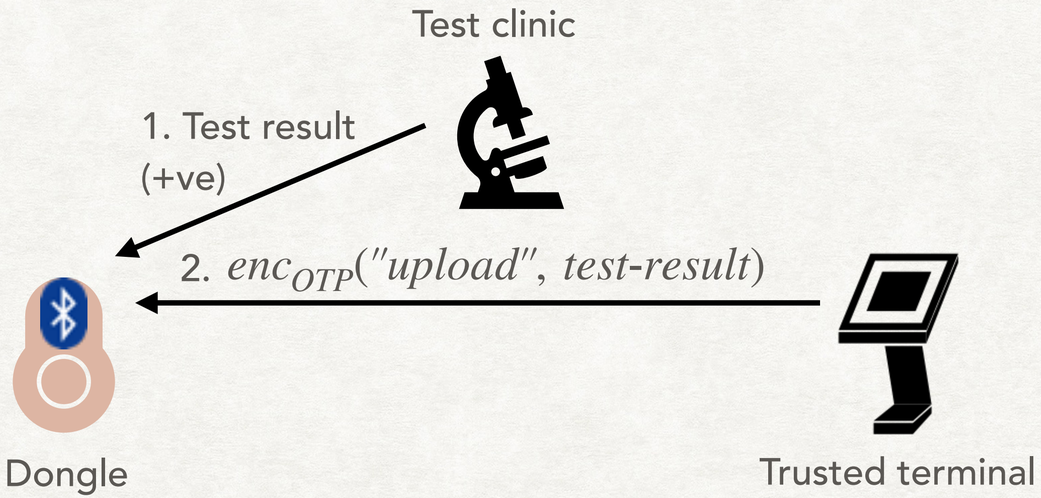
ENCOUNTER UPLOAD

1. Delayed release (using personal device)



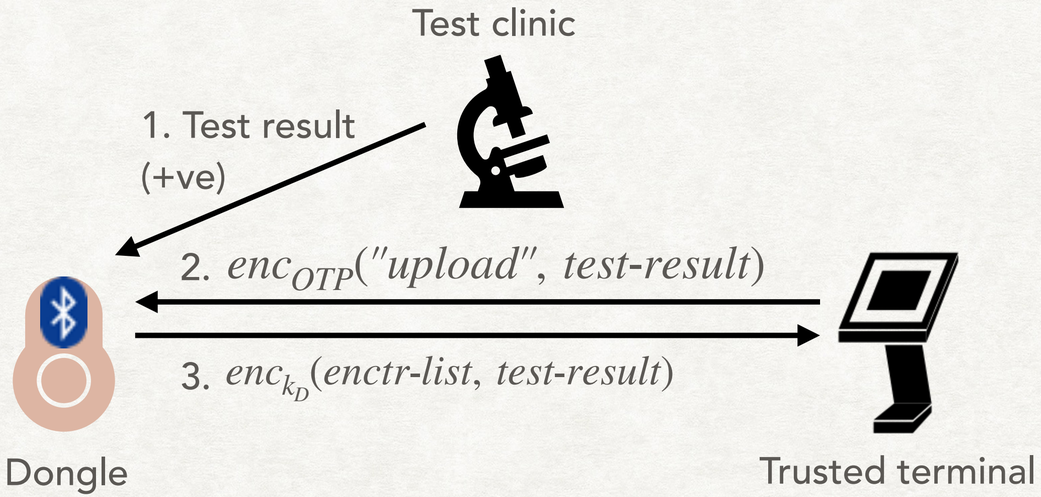
ENCOUNTER UPLOAD

1. Delayed release (using personal device)



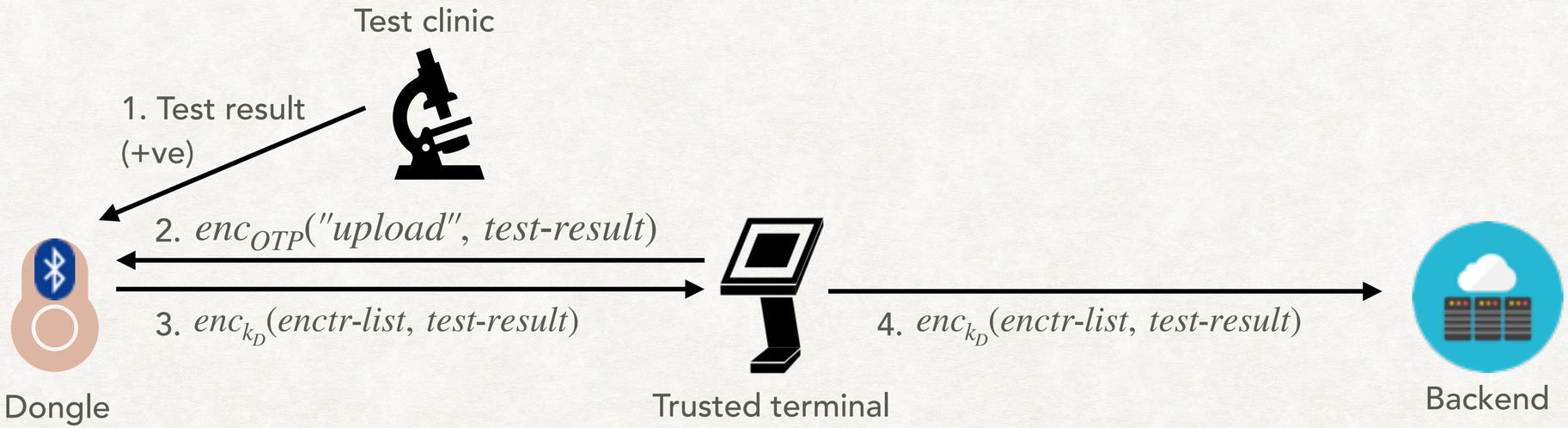
ENCOUNTER UPLOAD

1. Delayed release (using personal device)



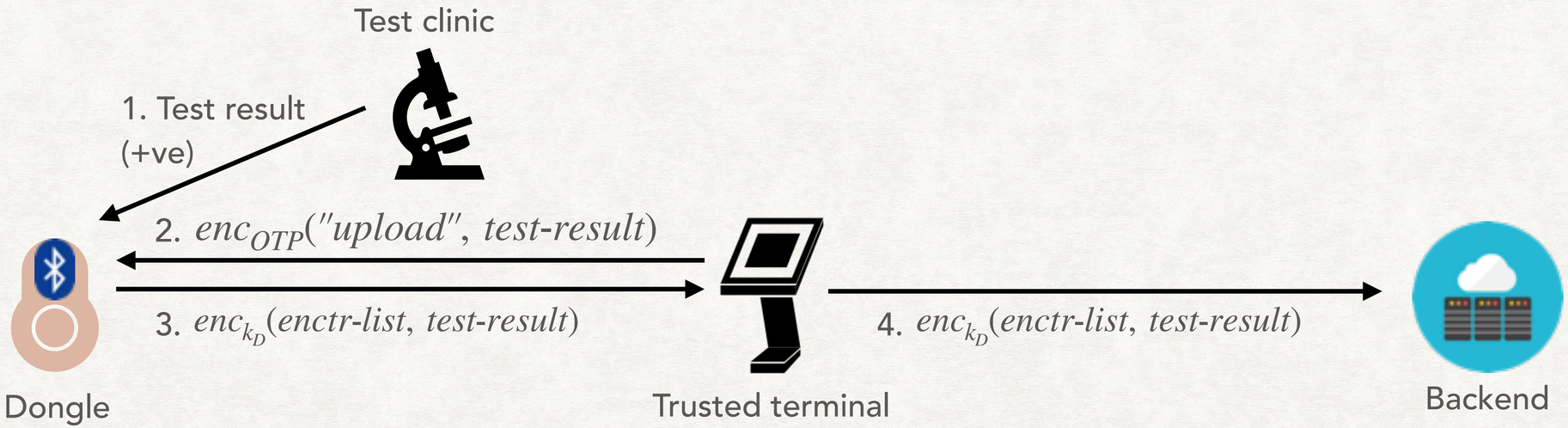
ENCOUNTER UPLOAD

1. Delayed release (using personal device)



ENCOUNTER UPLOAD

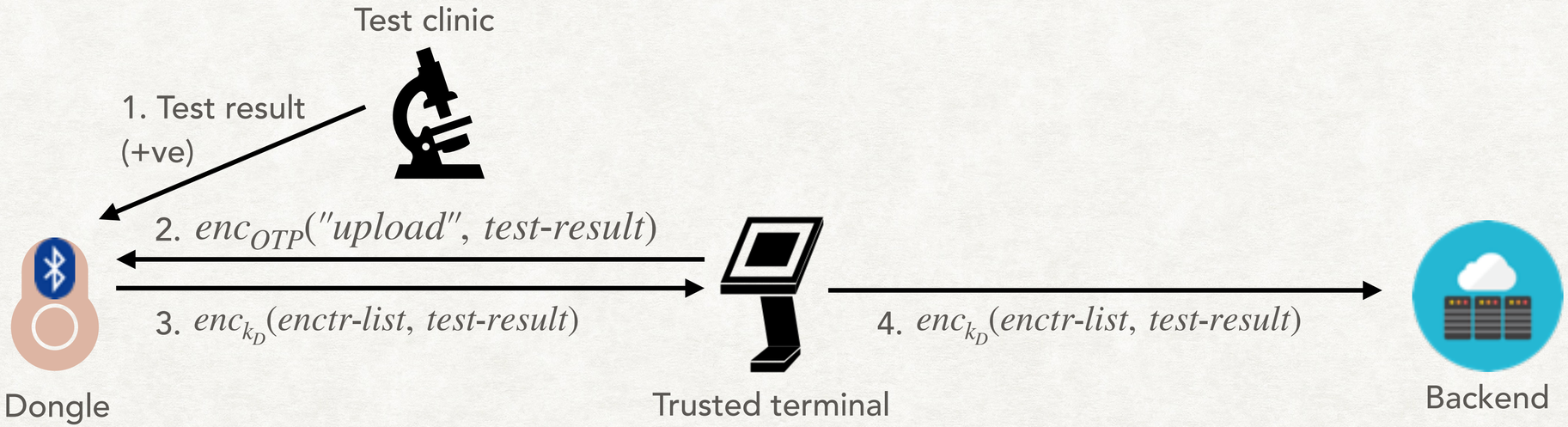
1. Delayed release (using personal device)



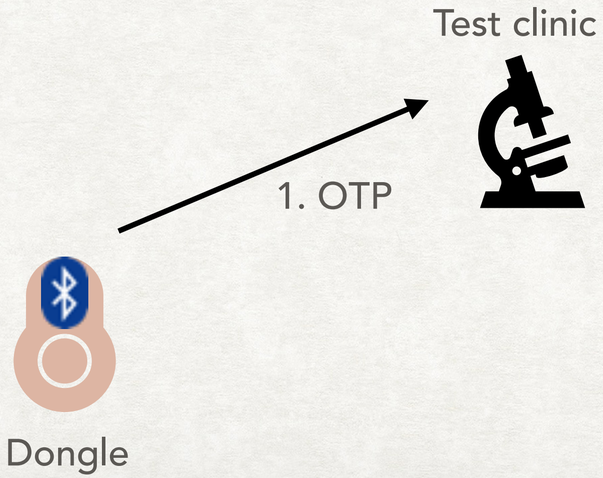
2. Early release (from test clinic)

ENCOUNTER UPLOAD

1. Delayed release (using personal device)

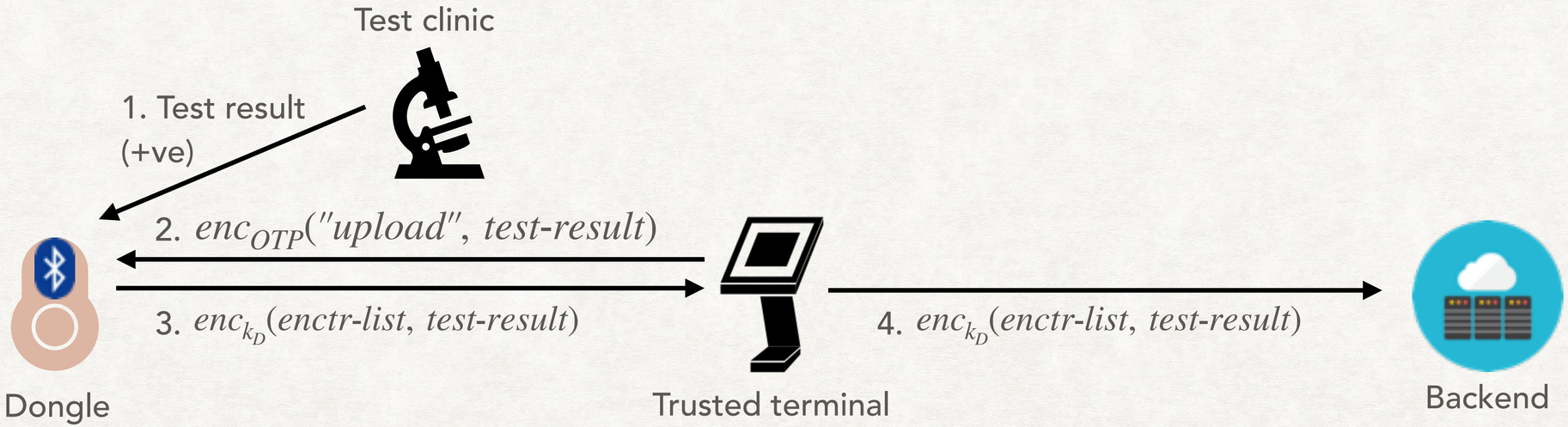


2. Early release (from test clinic)

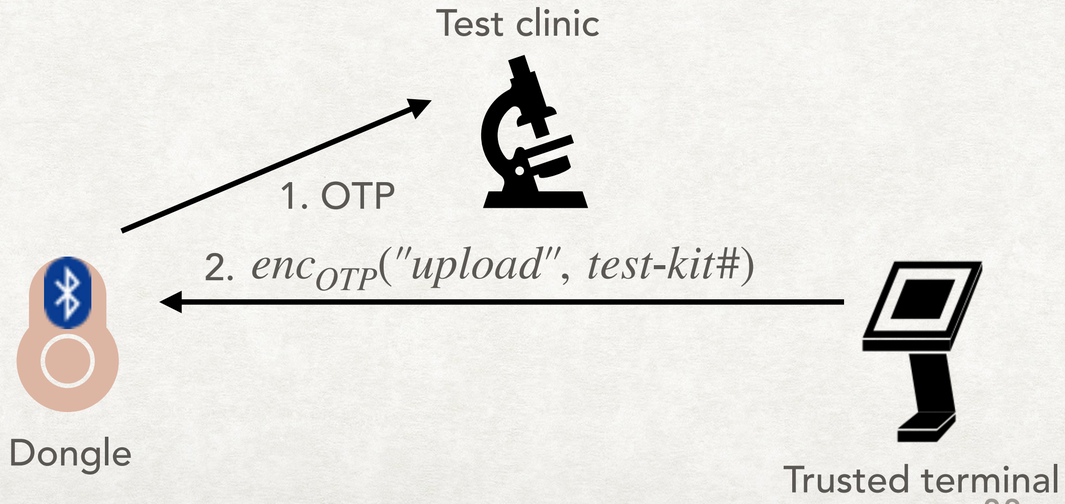


ENCOUNTER UPLOAD

1. Delayed release (using personal device)

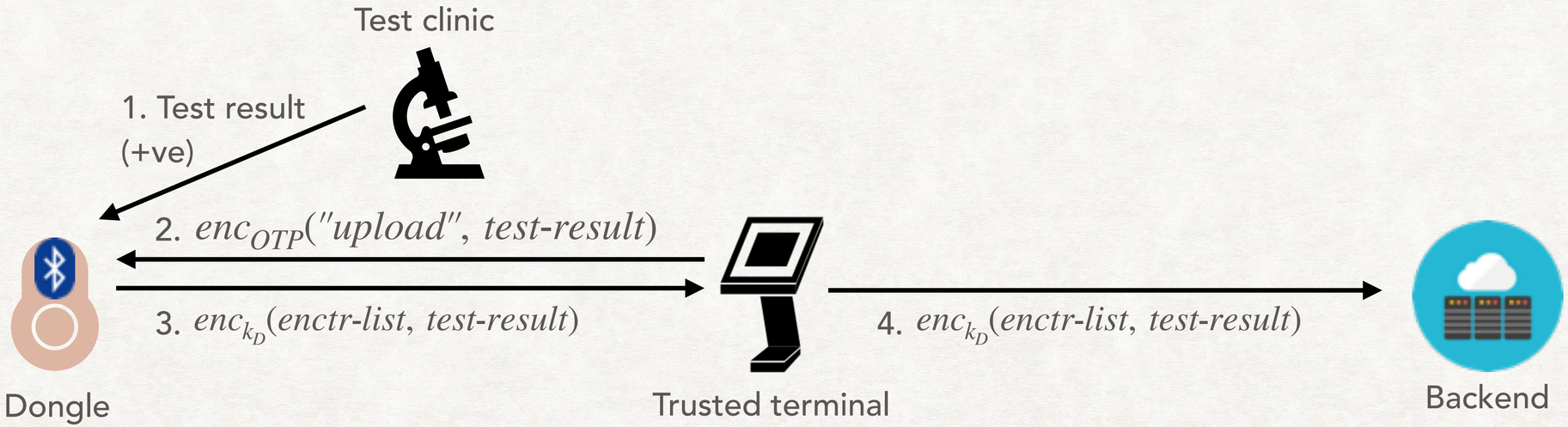


2. Early release (from test clinic)

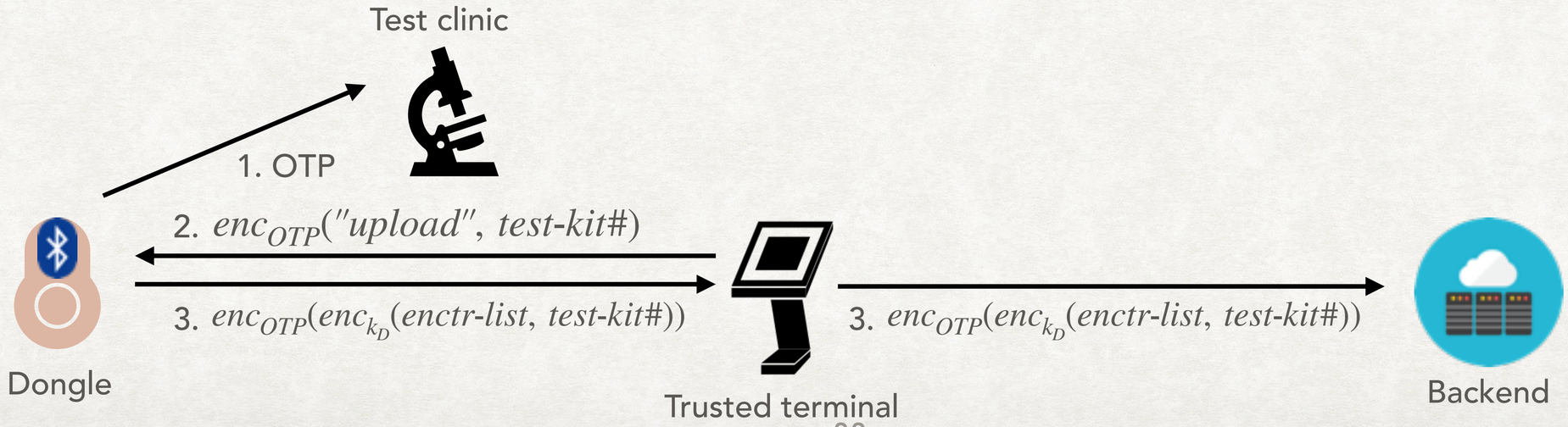


ENCOUNTER UPLOAD

1. Delayed release (using personal device)

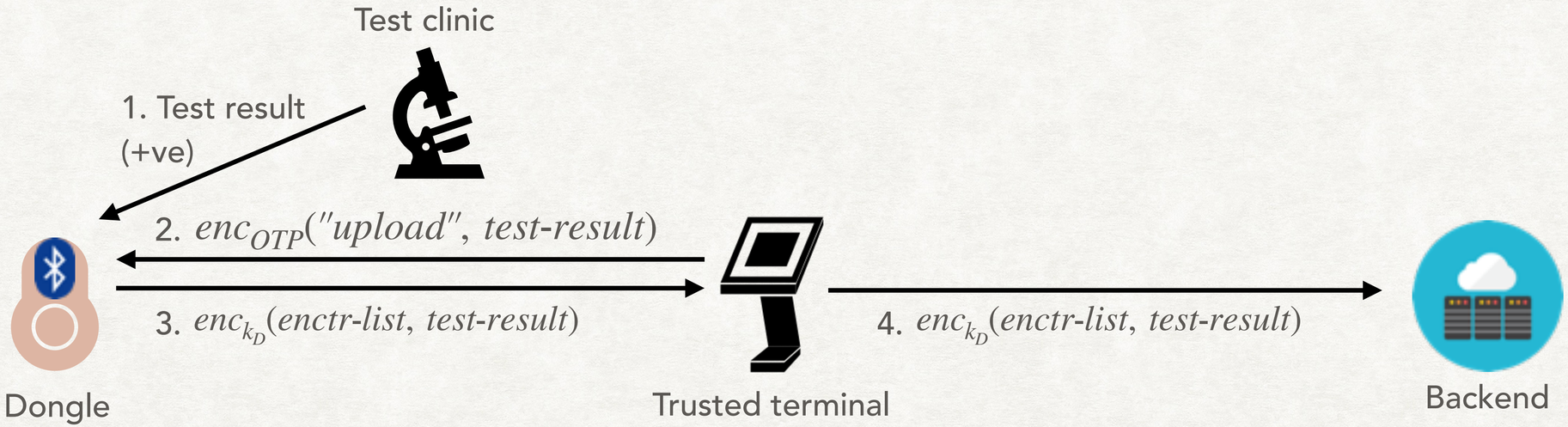


2. Early release (from test clinic)

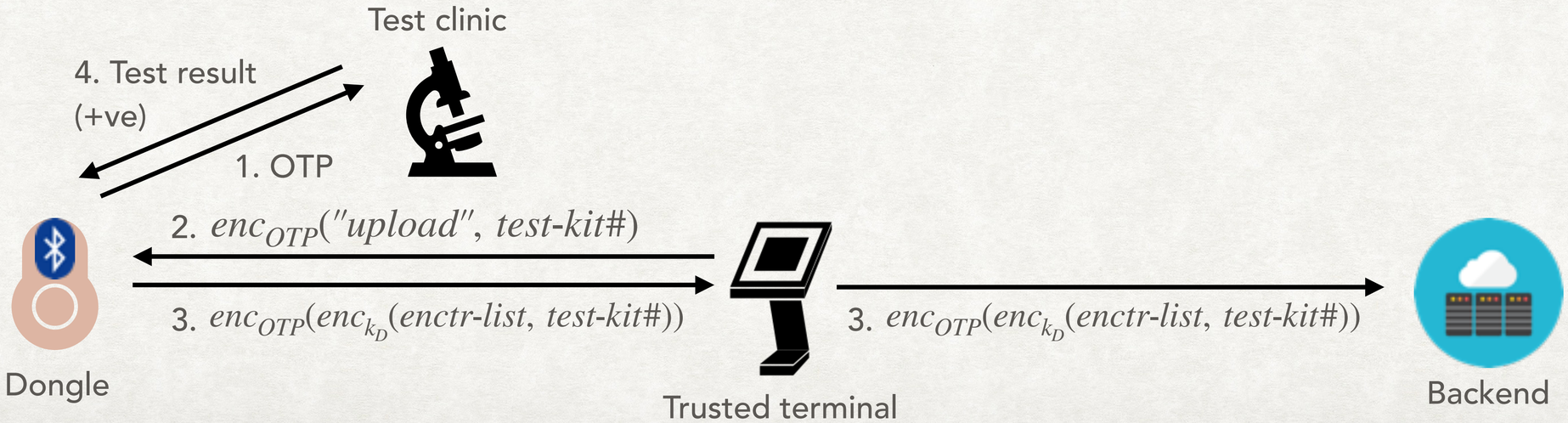


ENCOUNTER UPLOAD

1. Delayed release (using personal device)

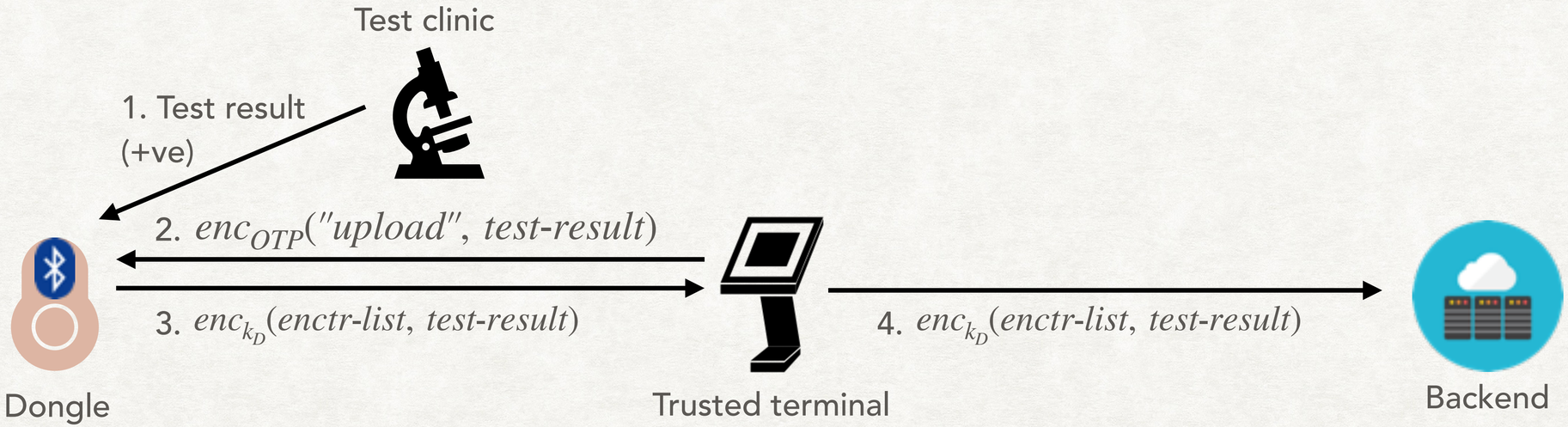


2. Early release (from test clinic)

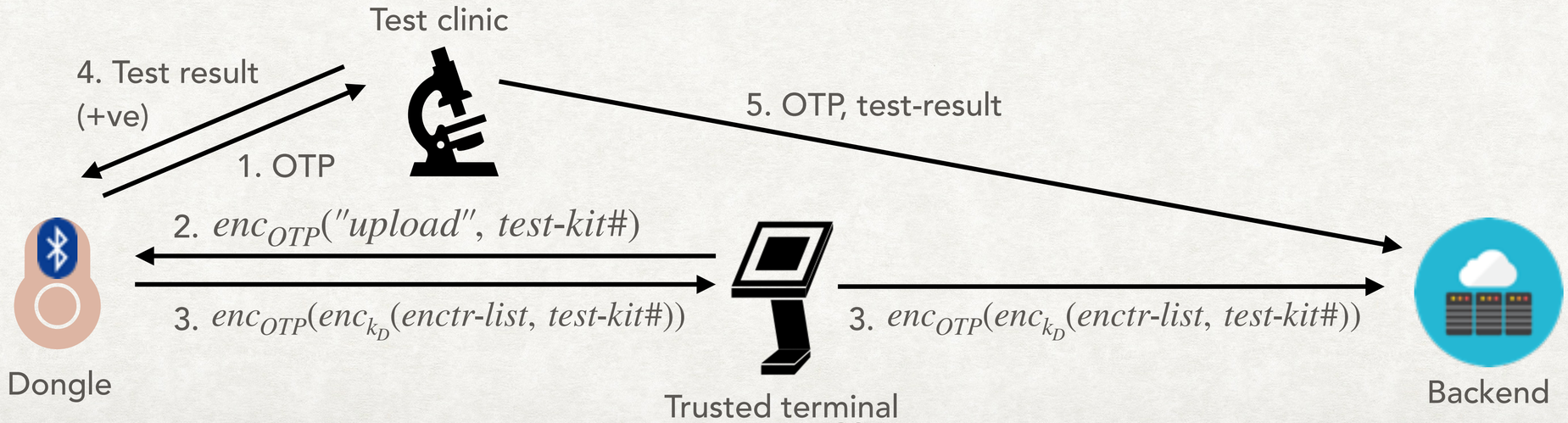


ENCOUNTER UPLOAD

1. Delayed release (using personal device)

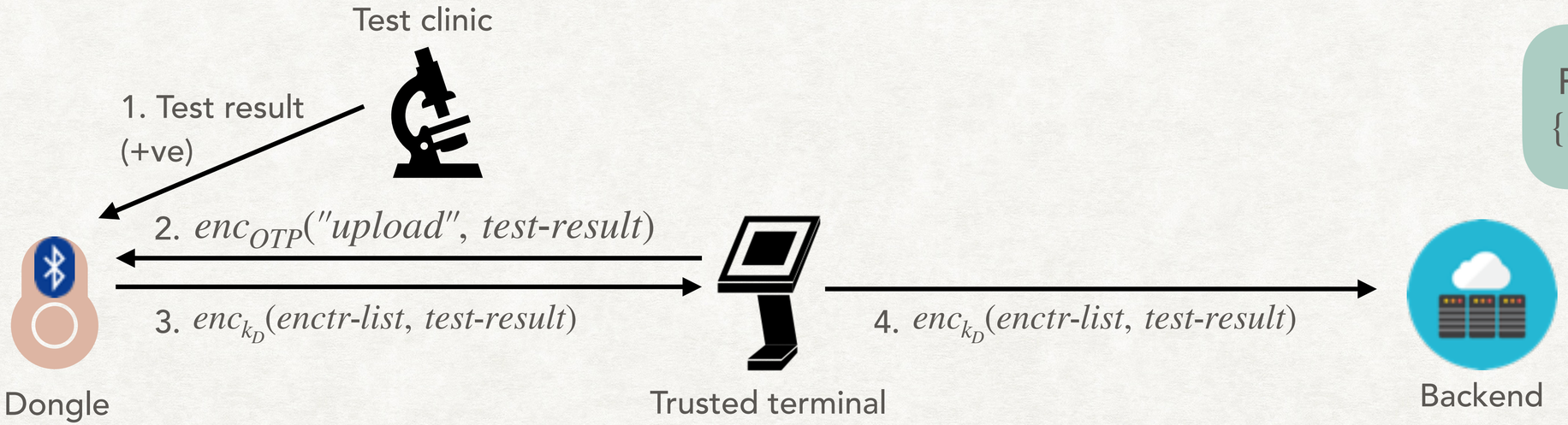


2. Early release (from test clinic)



ENCOUNTER UPLOAD

1. Delayed release (using personal device)



Risk database: $\{eph_{B,i_B}, loc_B, T\}$

2. Early release (from test clinic)