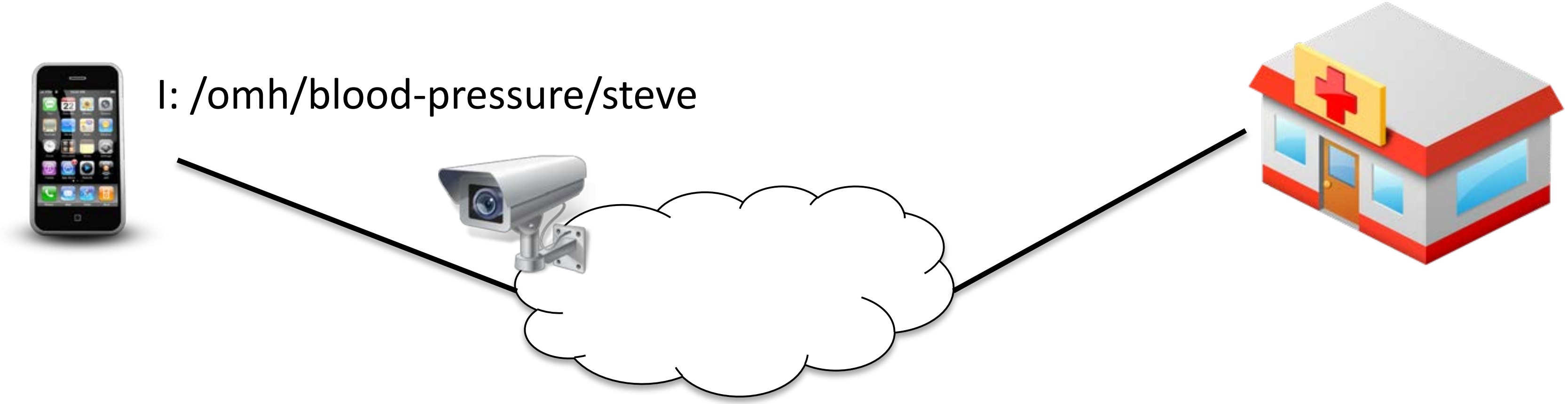
ANDaNA: Onion Routing for NDN

Steve DiBenedetto
Colorado State University

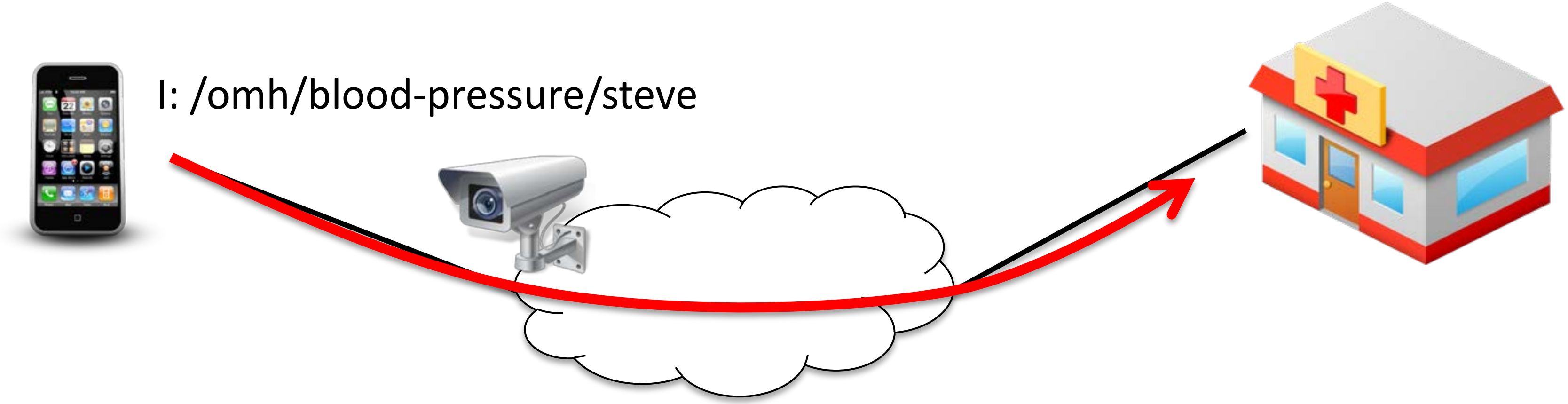
ANDaNA: Anonymous Named Data Networking Application
NDSS ’12
Steven DiBenedetto, Paolo Gasti, Gene Tsudik, Ersin Uzun

Information Linkage & Leakage

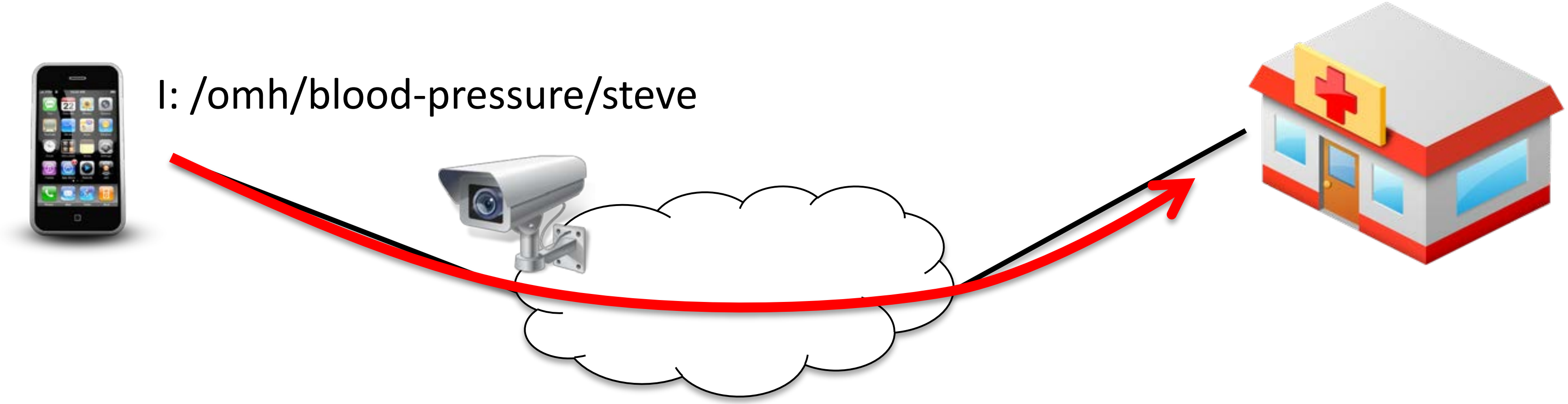


I: /omh/blood-pressure/steve

Information Linkage & Leakage

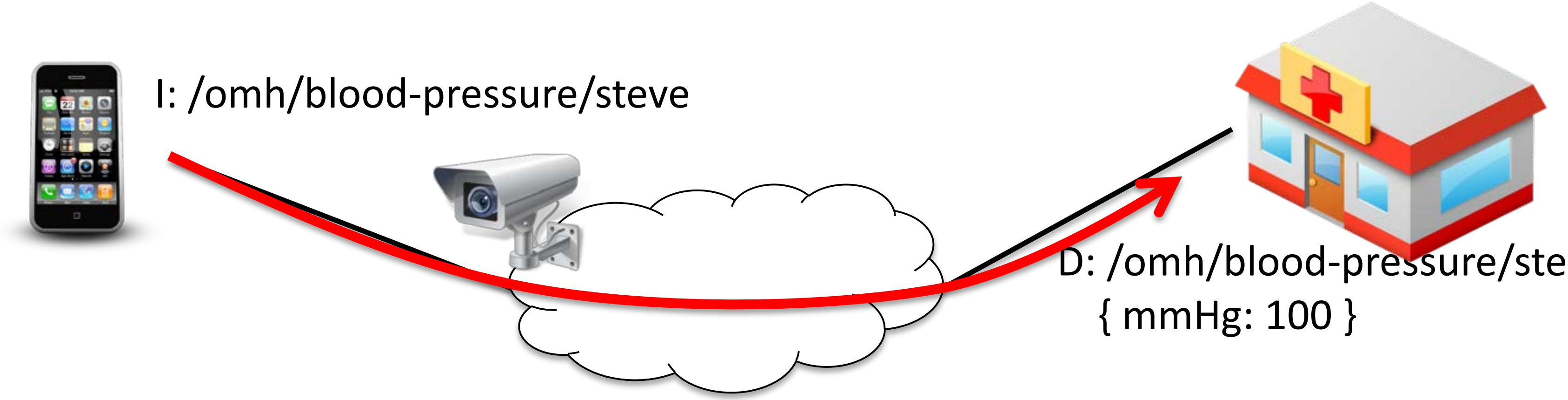


Information Linkage & Leakage



I: /omh/blood-pressure/steve

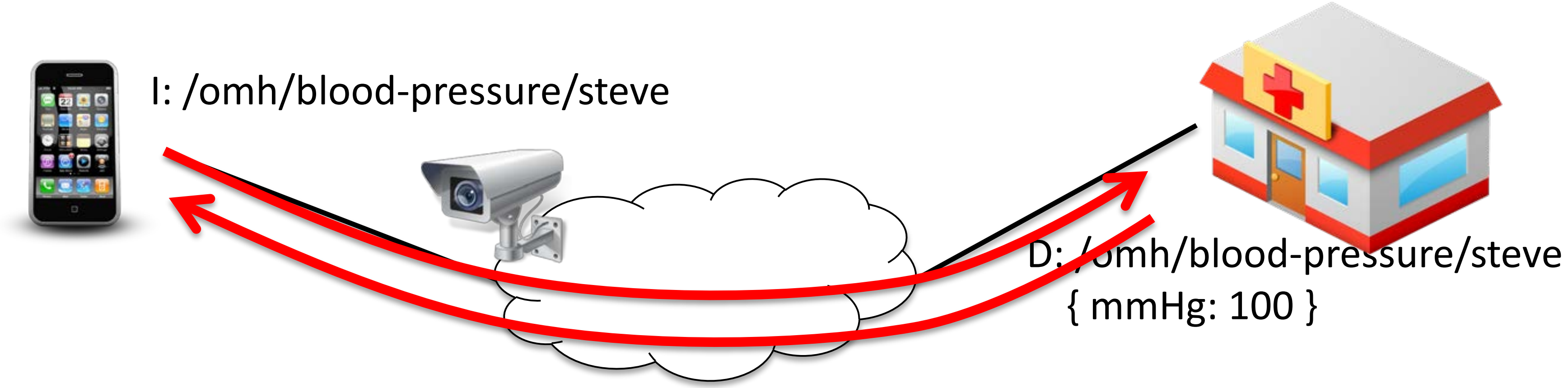
Information Linkage & Leakage



I: /omh/blood-pressure/steve

D: /omh/blood-pressure/steve
{ mmHg: 100 }

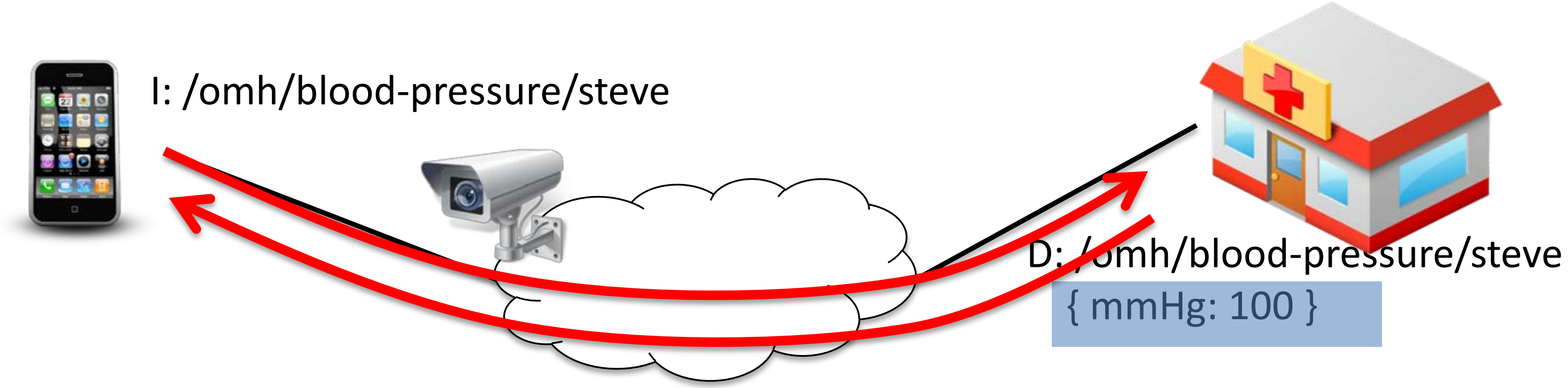
Information Linkage & Leakage



I: /omh/blood-pressure/steve

D: /omh/blood-pressure/steve
{ mmHg: 100 }

Information Linkage & Leakage

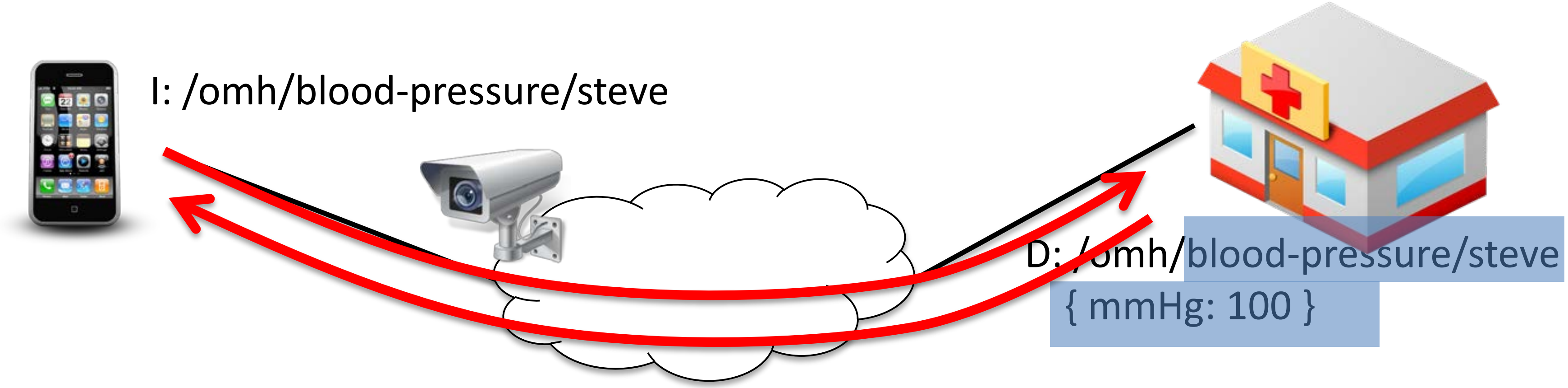


I: /omh/blood-pressure/steve

D: /omh/blood-pressure/steve

{ mmHg: 100 }

Information Linkage & Leakage

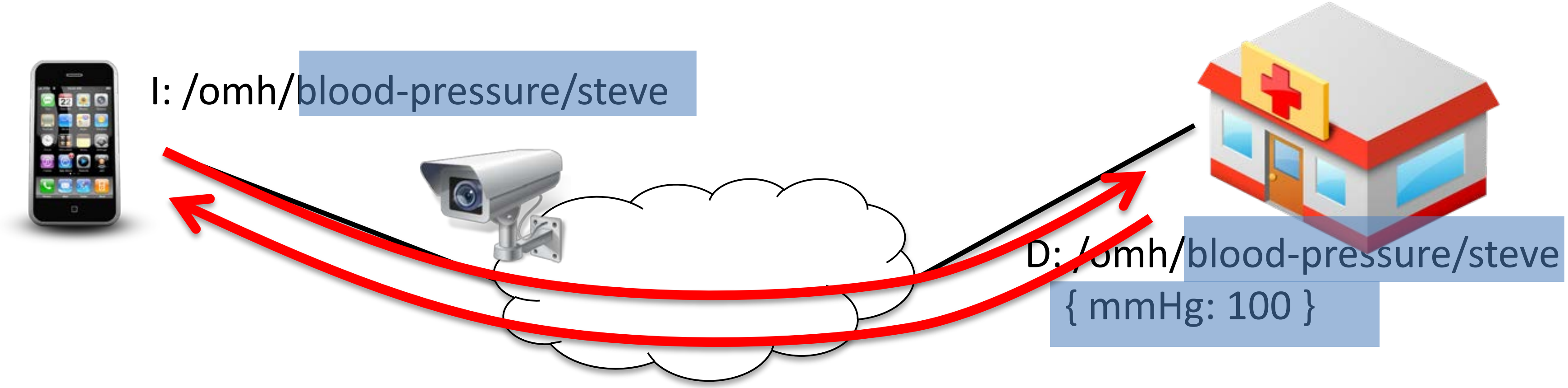


I: /omh/blood-pressure/steve

D: /omh/blood-pressure/steve

{ mmHg: 100 }

Information Linkage & Leakage

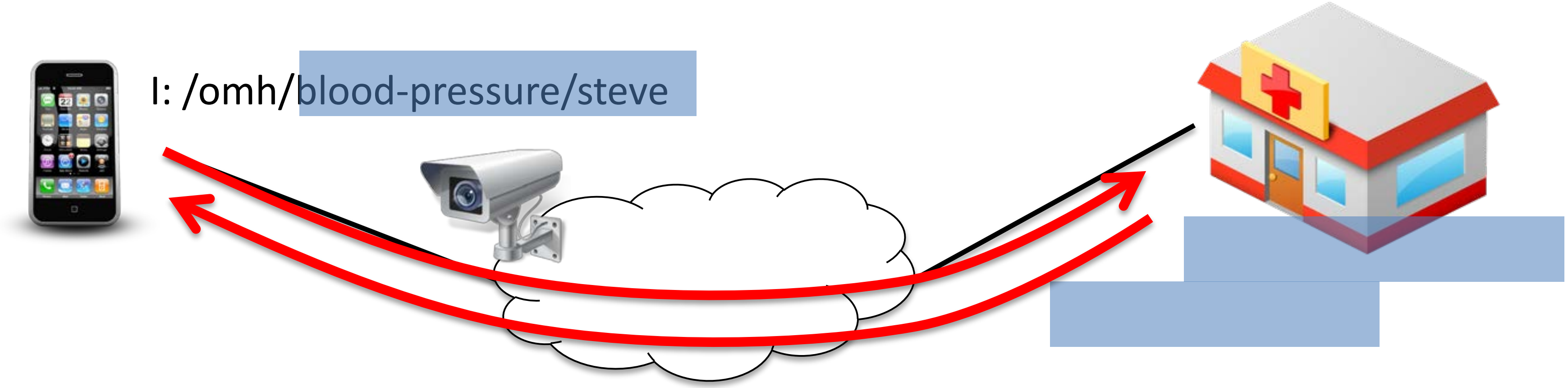


I: /omh/blood-pressure/steve

D: /omh/blood-pressure/steve

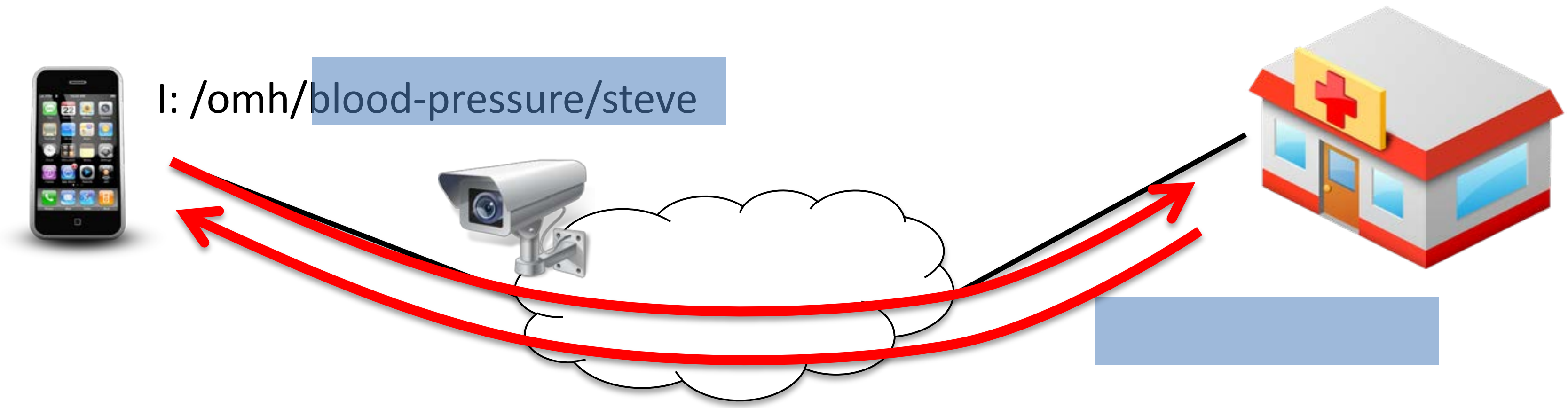
{ mmHg: 100 }

Information Linkage & Leakage



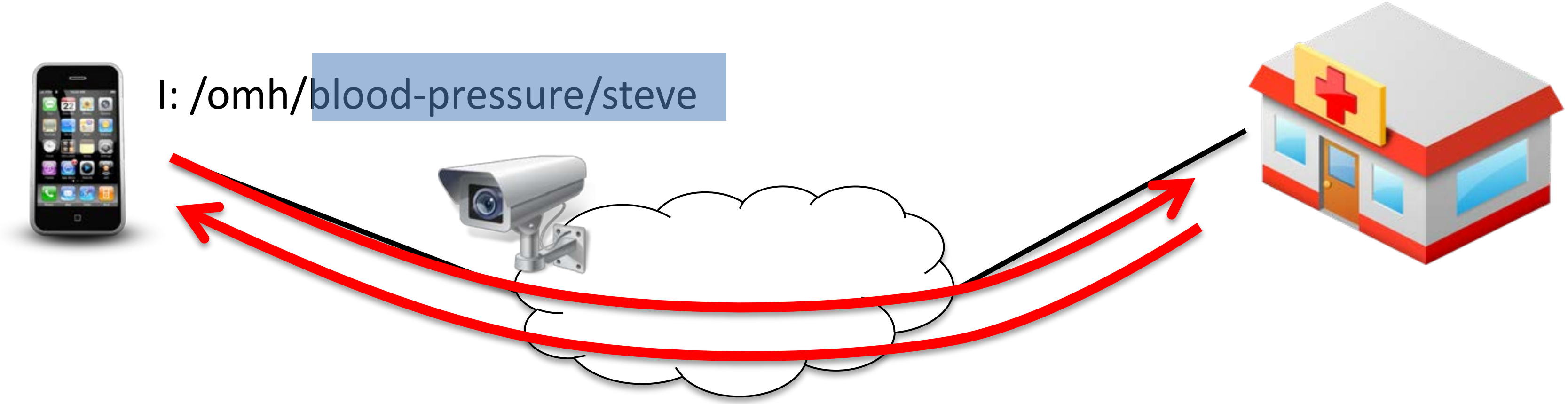
I: /omh/blood-pressure/steve

Information Linkage & Leakage



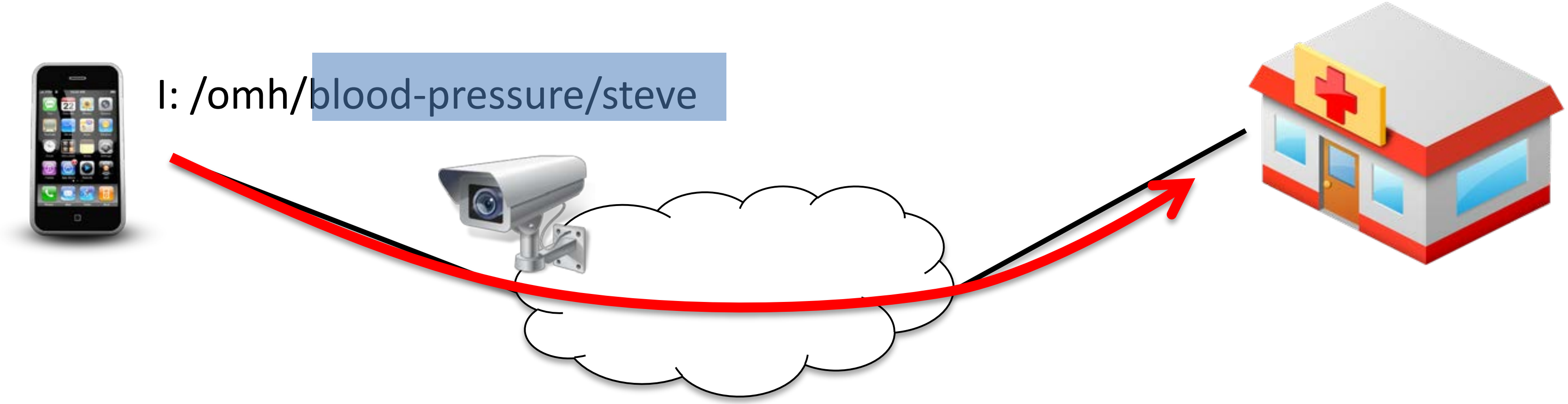
I: /omh/blood-pressure/steve

Information Linkage & Leakage

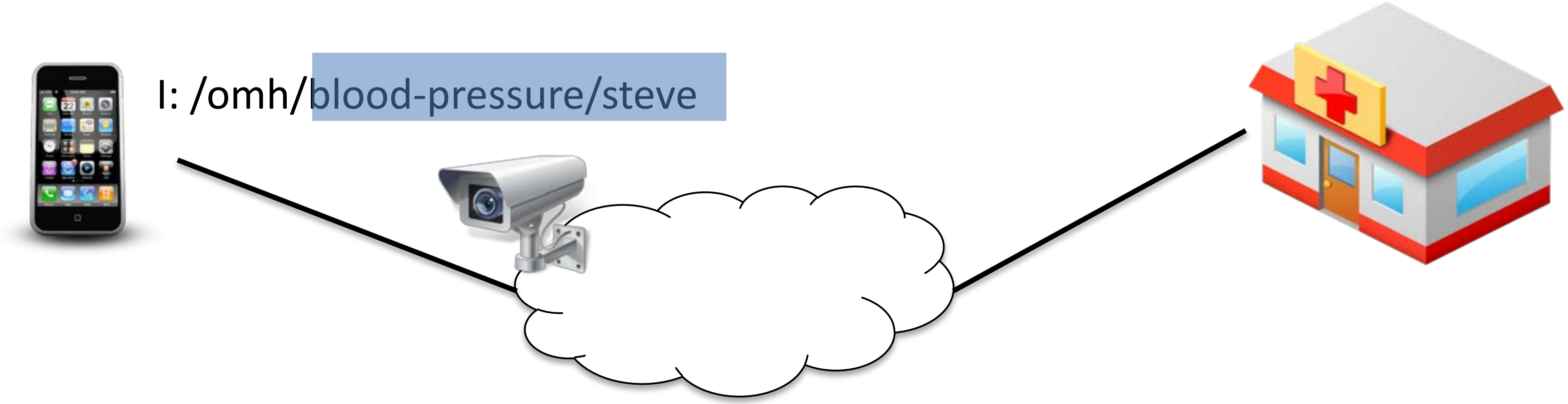


I: /omh/blood-pressure/steve

Information Linkage & Leakage

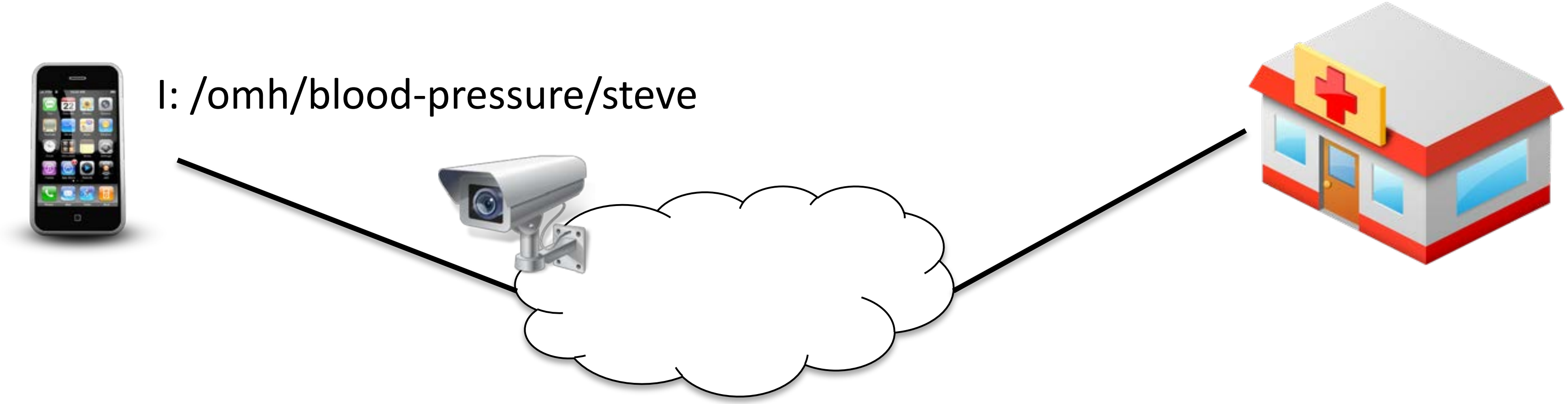


Information Linkage & Leakage



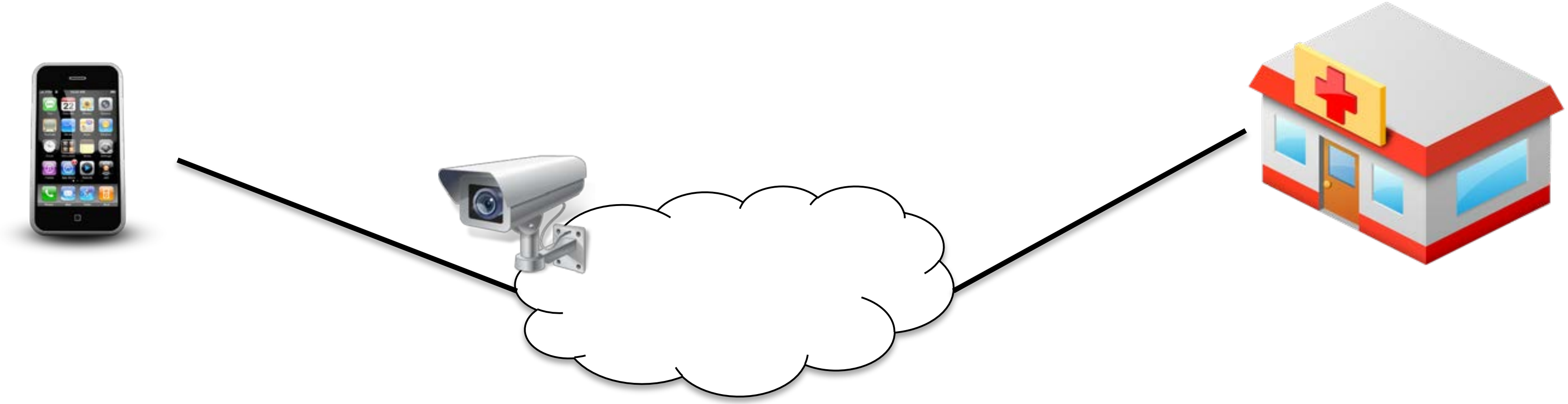
I: /omh/blood-pressure/steve

Information Linkage & Leakage

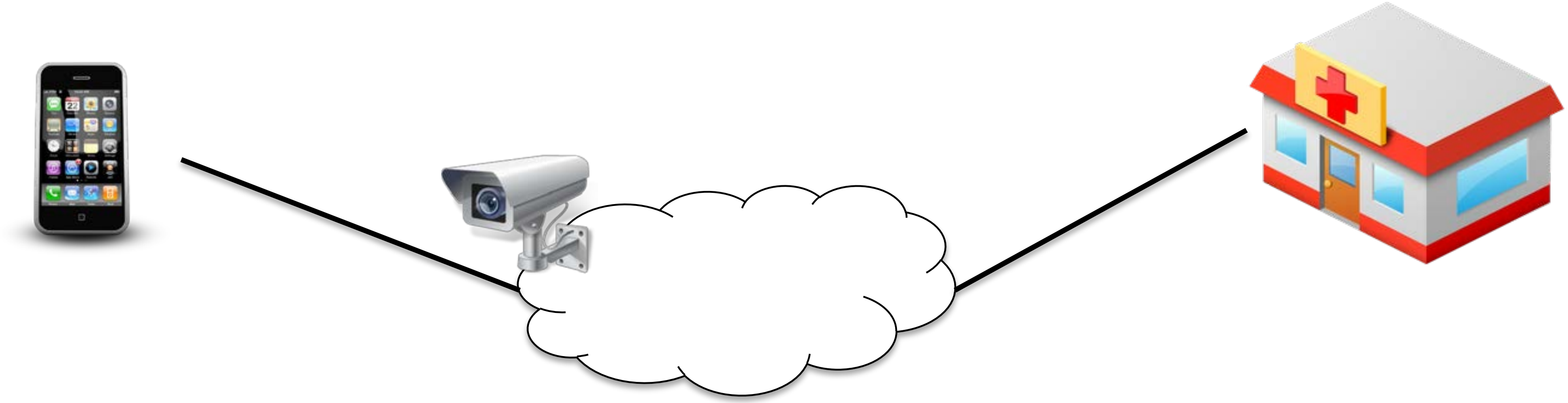


I: /omh/blood-pressure/steve

Information Linkage & Leakage

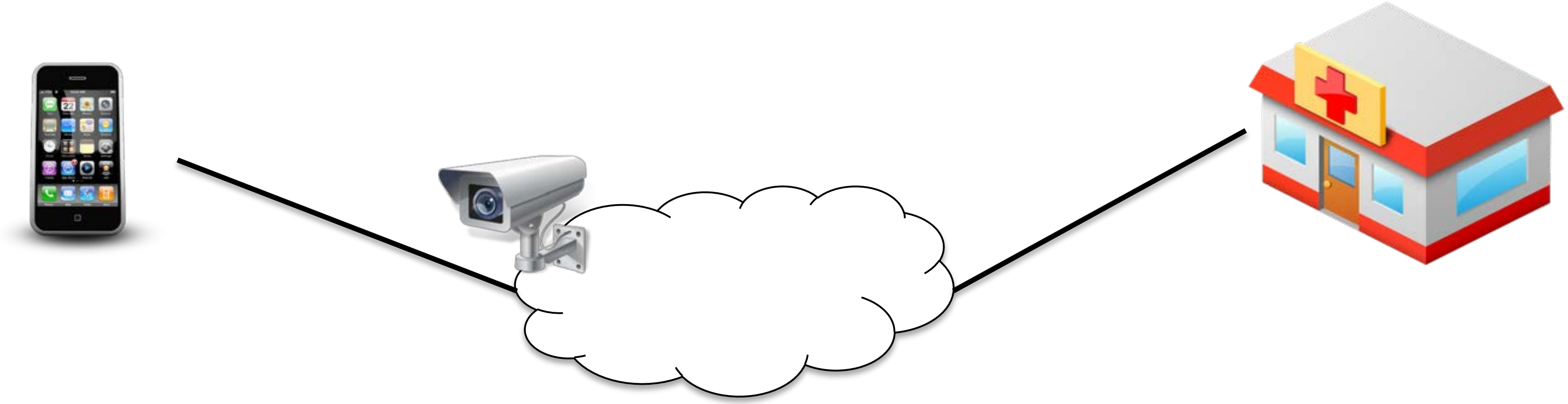


Information Linkage & Leakage



I: /omh/blood-pressure/steve
Nonce: <rand-int>
Lifetime: <int>
Loc: /fitbit/key

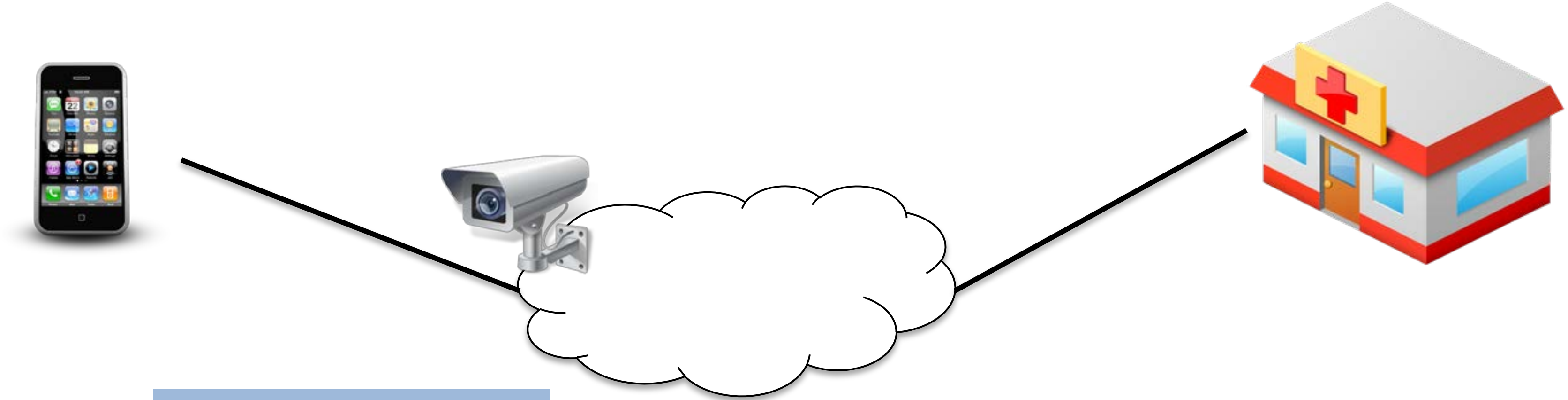
Information Linkage & Leakage



I: /omh/blood-pressure/steve
Nonce: <rand-int>
Lifetime: <int>
Loc: /fitbit/key

D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

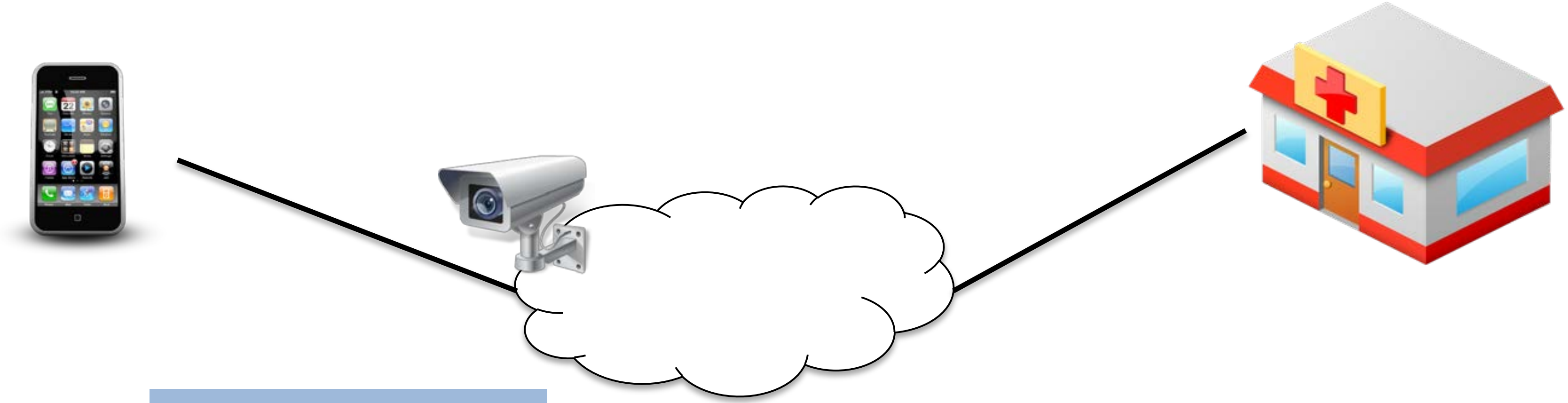
Information Linkage & Leakage



I: /omh/blood-pressure/steve
Nonce: <rand-int>
Lifetime: <int>
Loc: /fitbit/key

D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

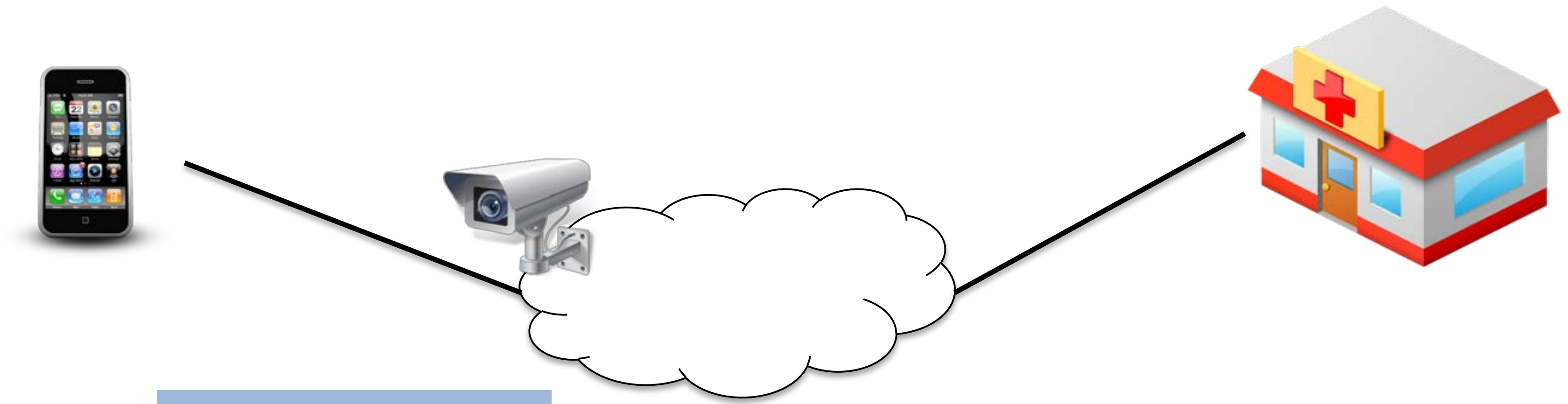
Information Linkage & Leakage



I: /omh/blood-pressure/steve
Nonce: <rand-int>
Lifetime: <int>
Loc: /fitbit/key

D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

Information Linkage & Leakage

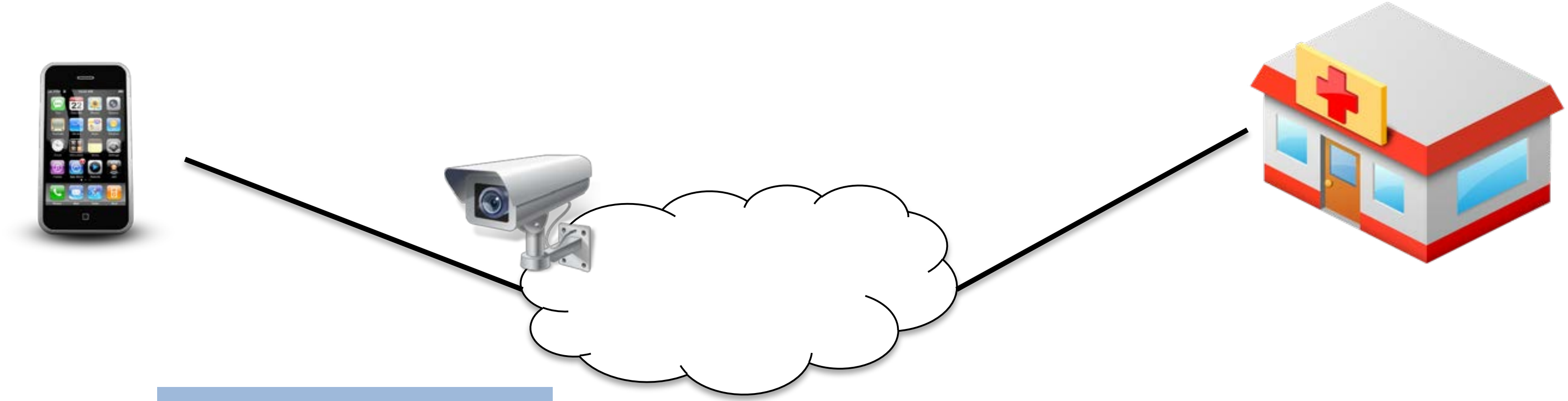


I: /omh/blood-pressure/steve

Nonce: <rand-int>
Lifetime: <int>
Loc: /fitbit/key

D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

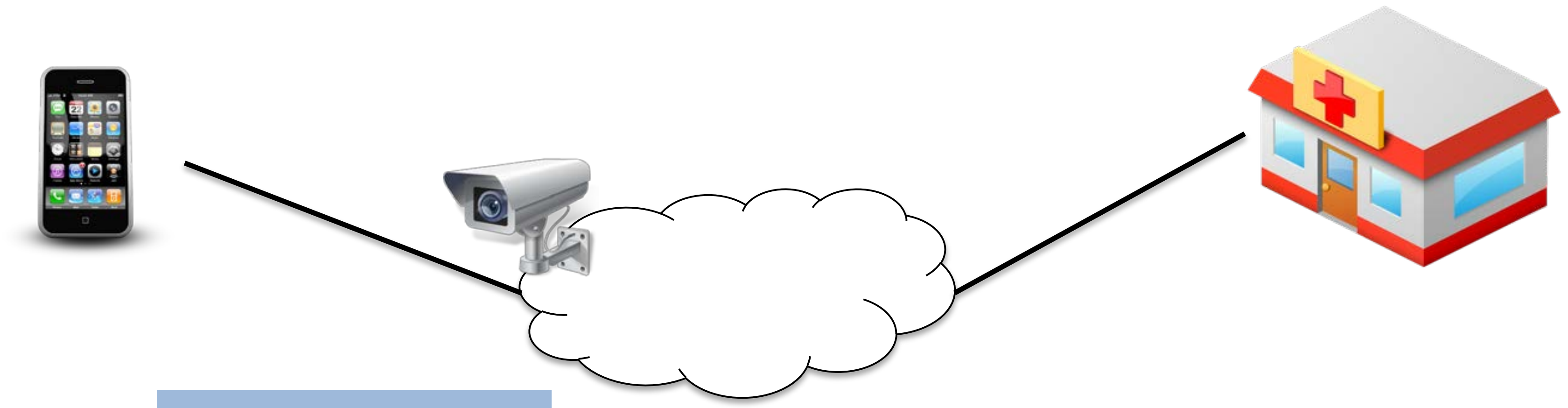
Information Linkage & Leakage



I: /omh/blood-pressure/steve
Nonce: <rand-int>
Lifetime: <int>
Loc: /fitbit/key

D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

Information Linkage & Leakage

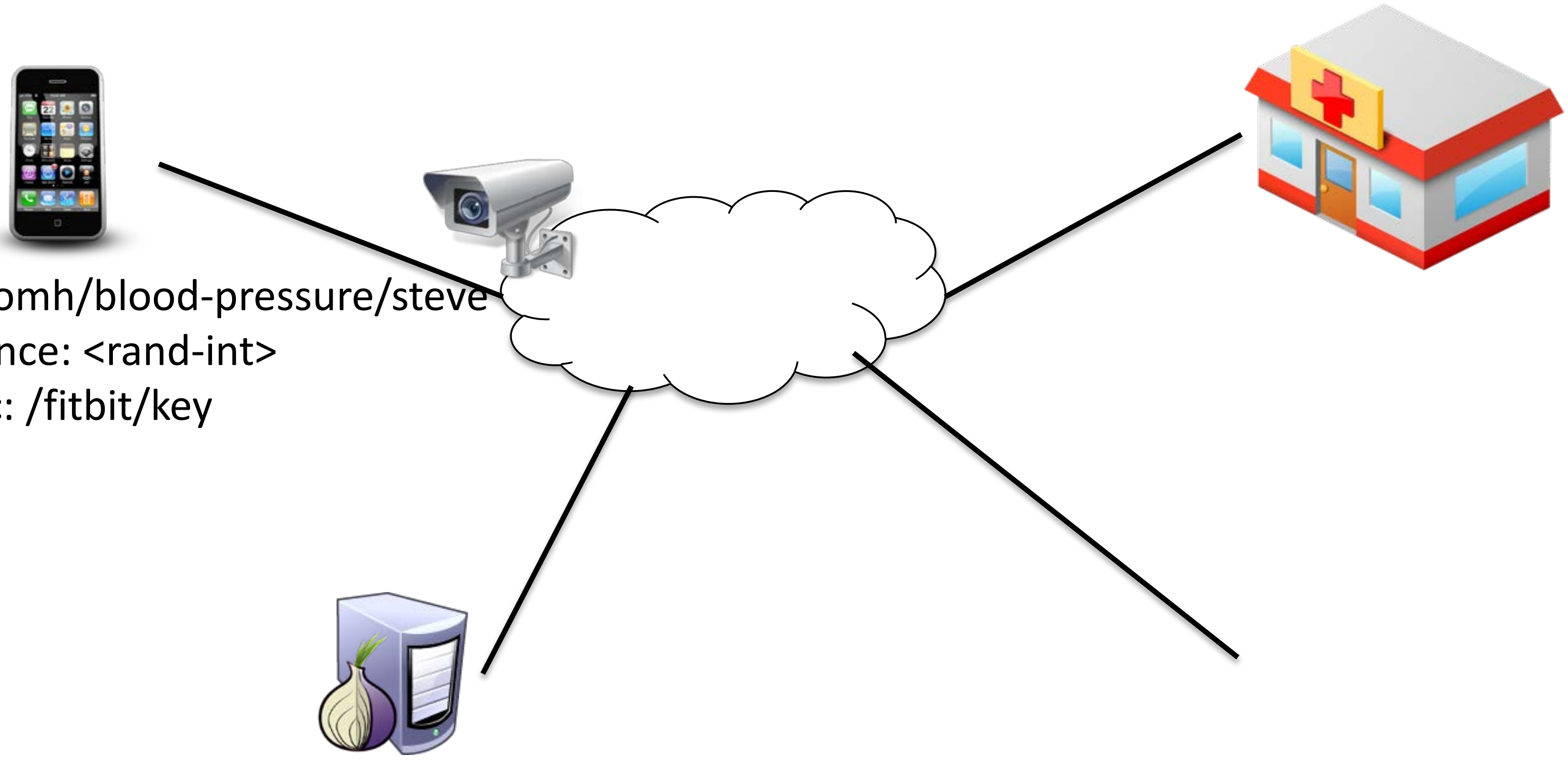


I: /omh/blood-pressure/steve
Nonce: <rand-int>
Lifetime: <int>
Loc: /fitbit/key

D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

- Encrypted names, payloads, and header fields may link requester to sensitive content or leak information

Onion Routing in NDN

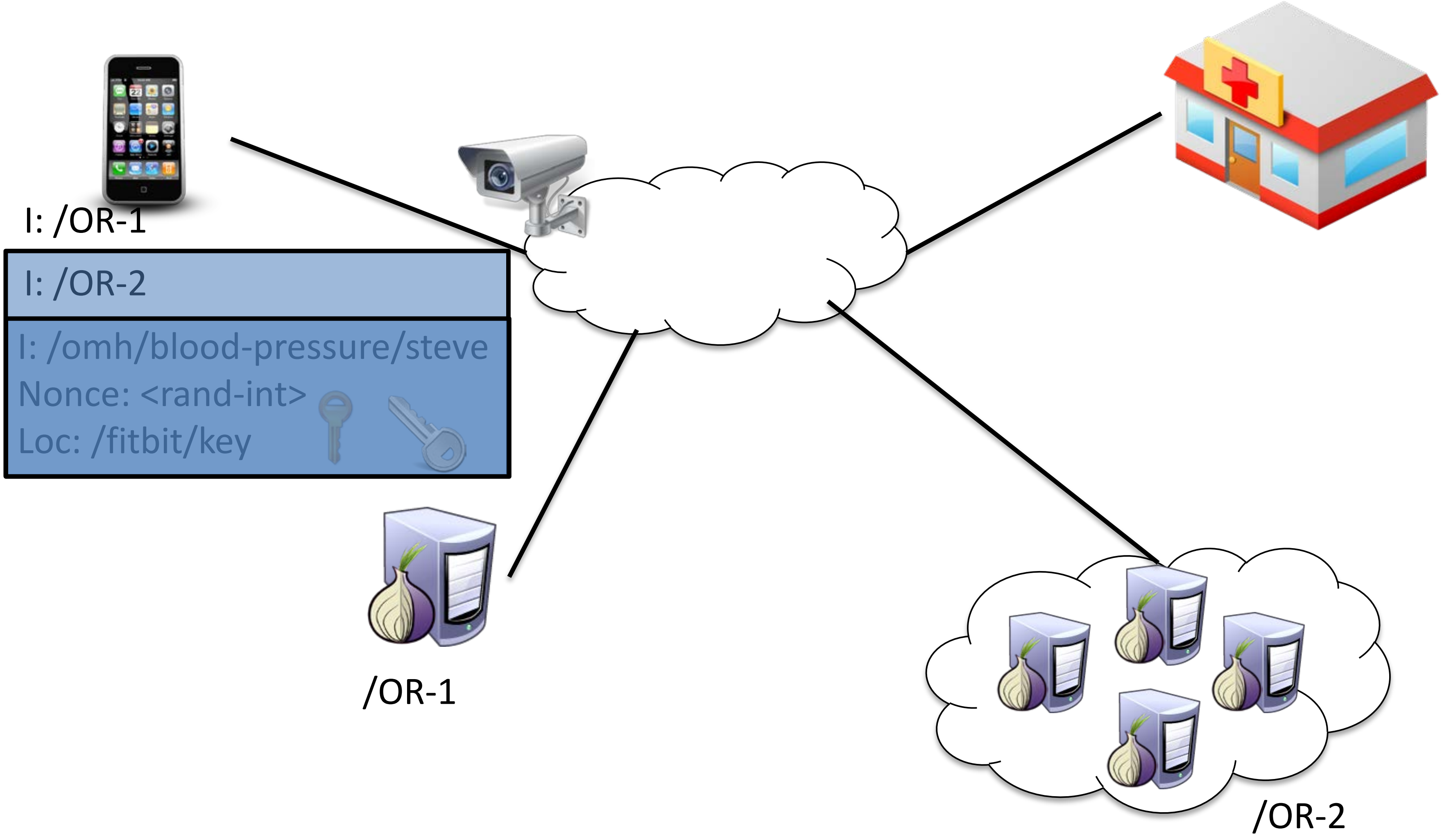


I: /omh/blood-pressure/steve
Nonce: <rand-int>
Loc: /fitbit/key

/OR-1

/OR-2

Onion Routing in NDN



I: /OR-1

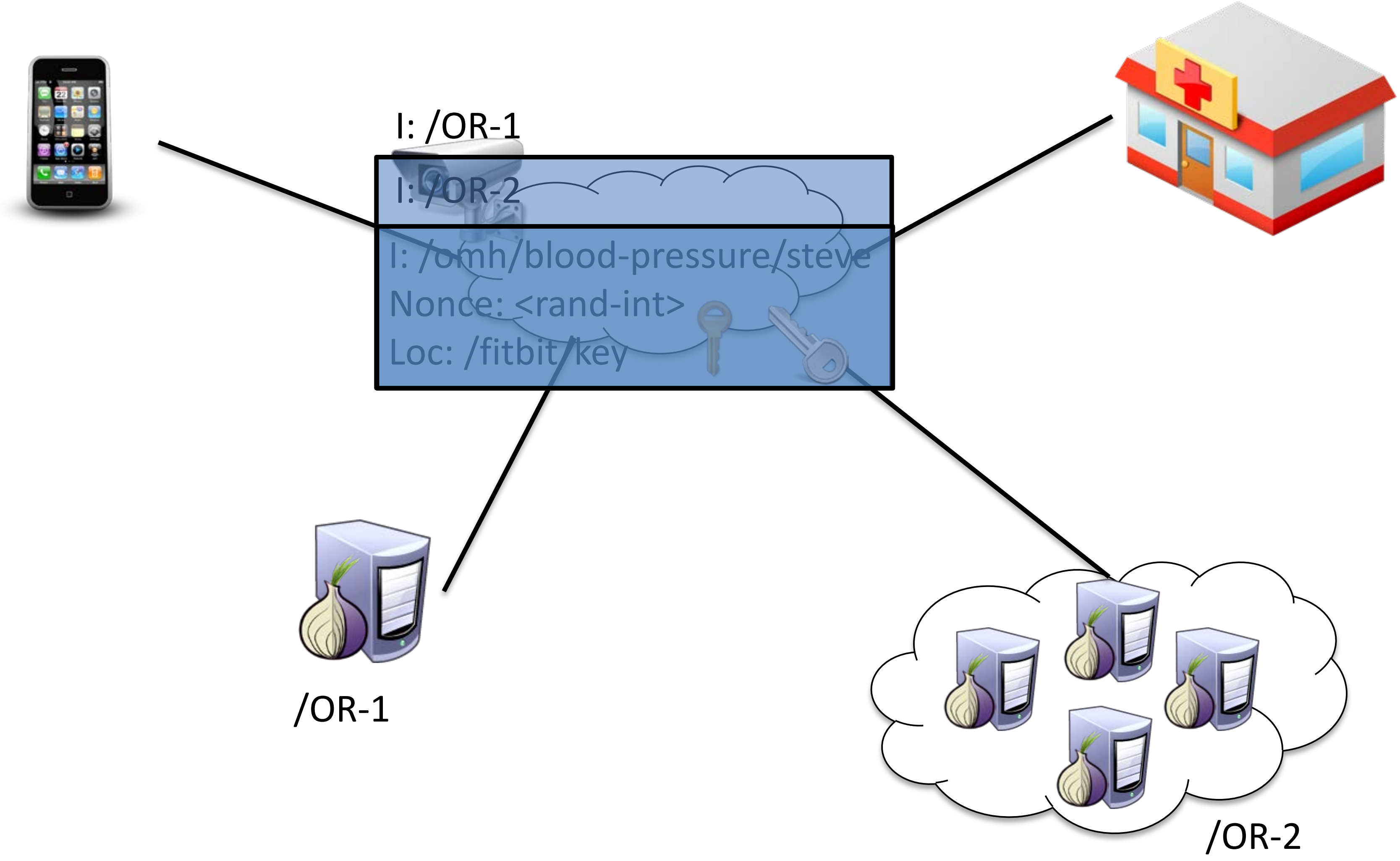
I: /OR-2

I: /omh/blood-pressure/steve
Nonce: <rand-int>
Loc: /fitbit/key

/OR-1

/OR-2

Onion Routing in NDN



I: /OR-1

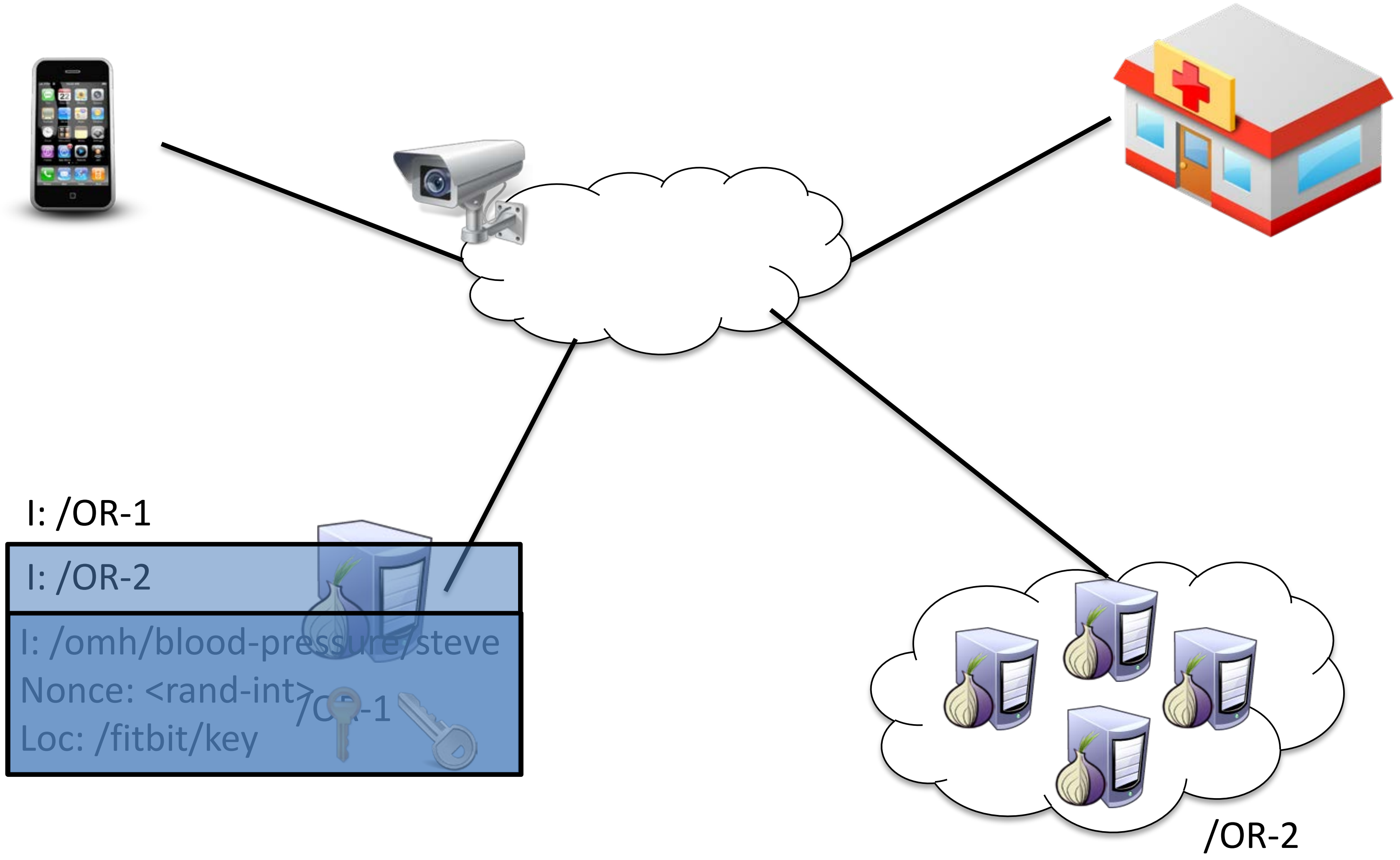
I: /OR-2

I: /omh/blood-pressure/steve
Nonce: <rand-int>
Loc: /fitbit/key

/OR-1

/OR-2

Onion Routing in NDN

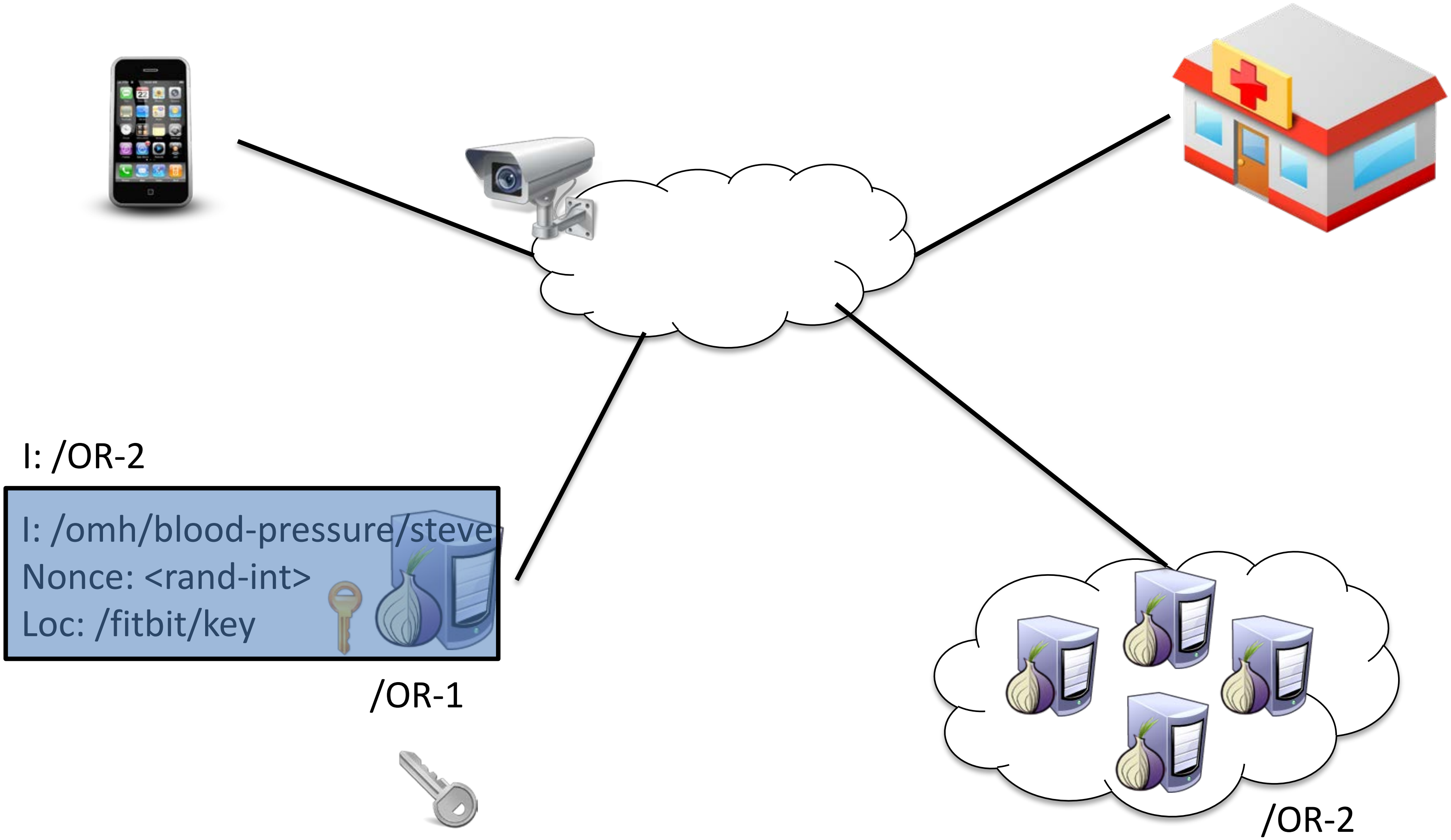


I: /OR-1

I: /OR-2

I: /omh/blood-pressure/steve
Nonce: <rand-int>
Loc: /fitbit/key

Onion Routing in NDN



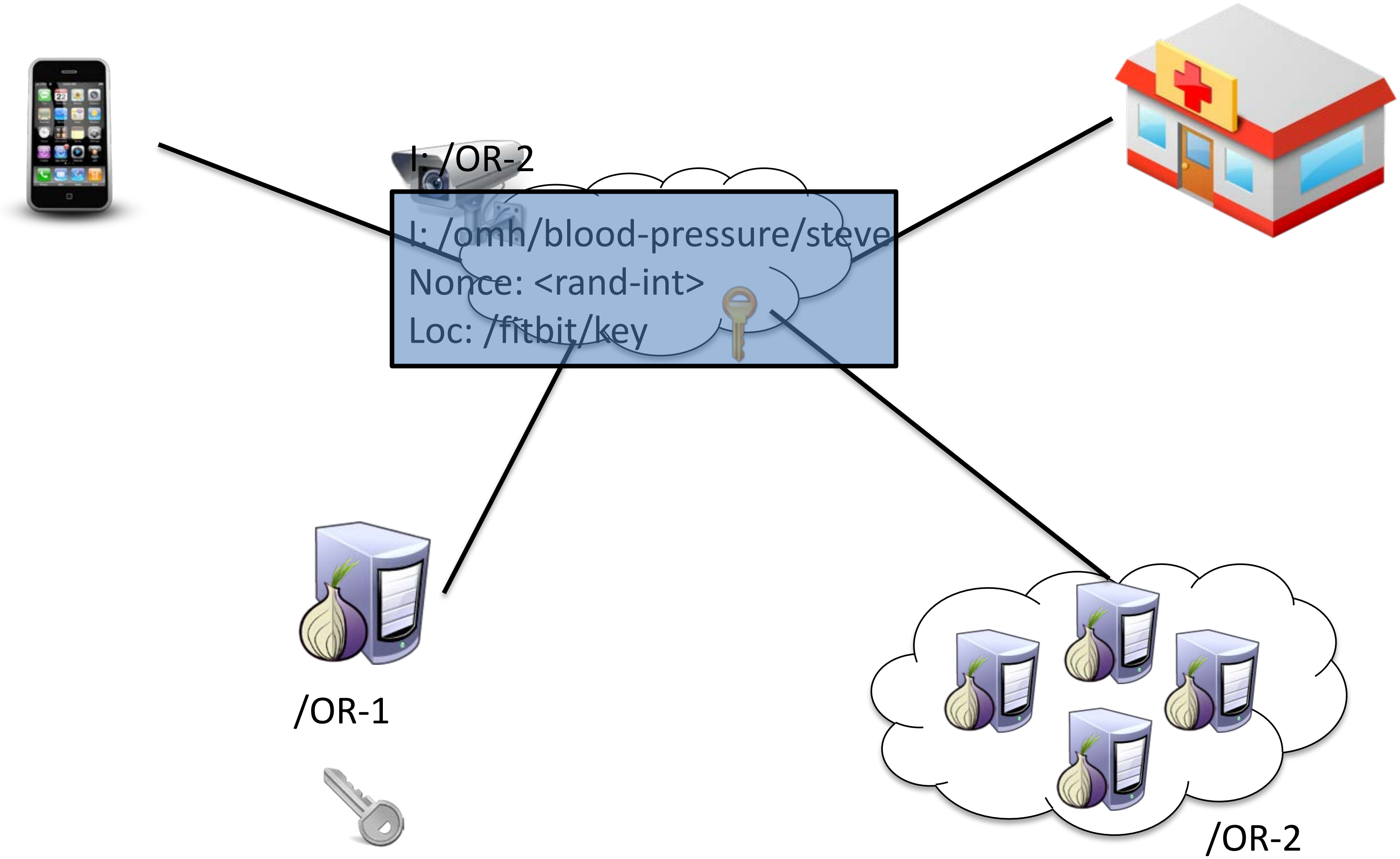
I: /OR-2

I: /omh/blood-pressure/steve
Nonce: <rand-int>
Loc: /fitbit/key

/OR-1

/OR-2

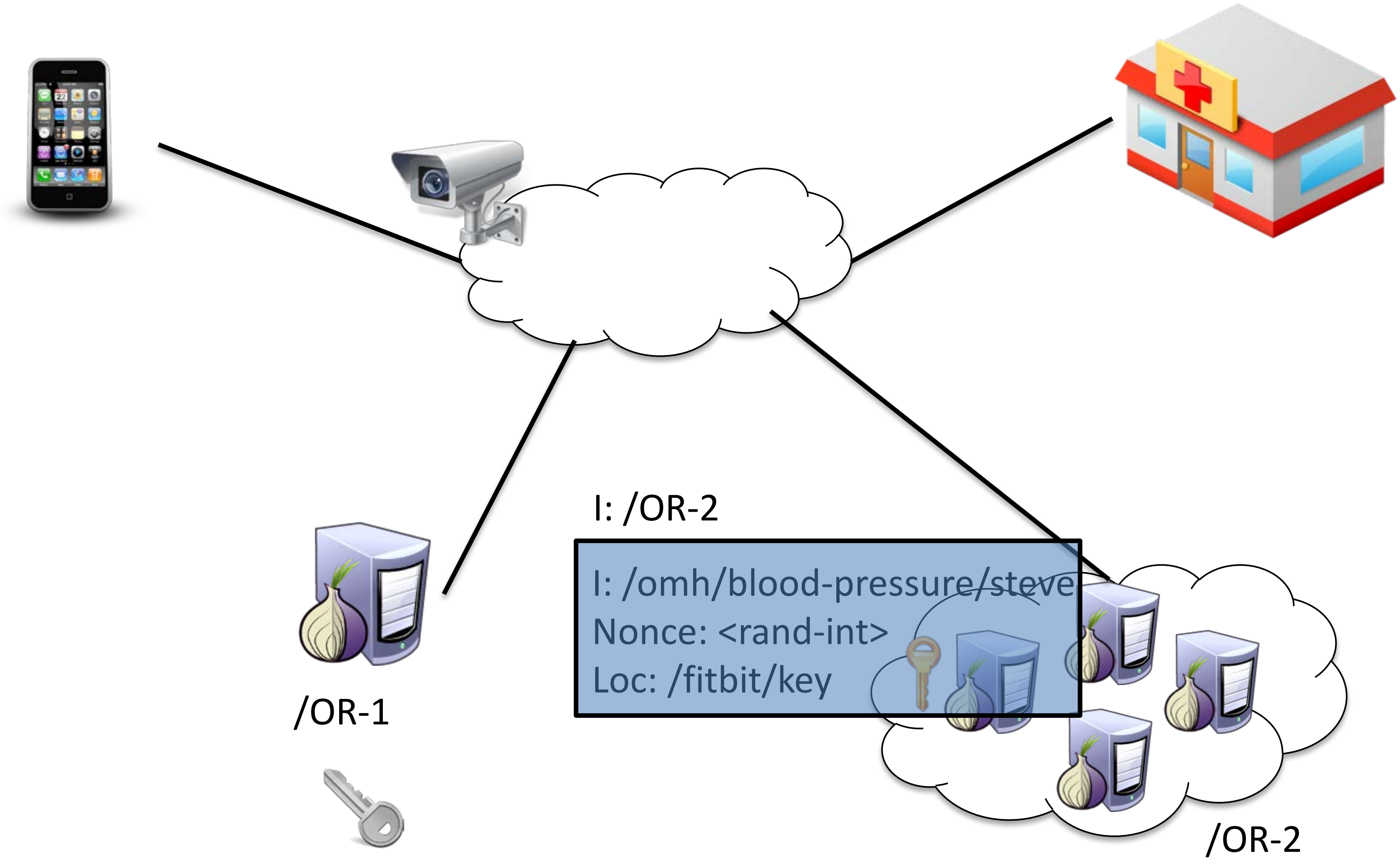
Onion Routing in NDN



I: /OR-2

I: /omh/blood-pressure/steve
Nonce: <rand-int>
Loc: /fitbit/key

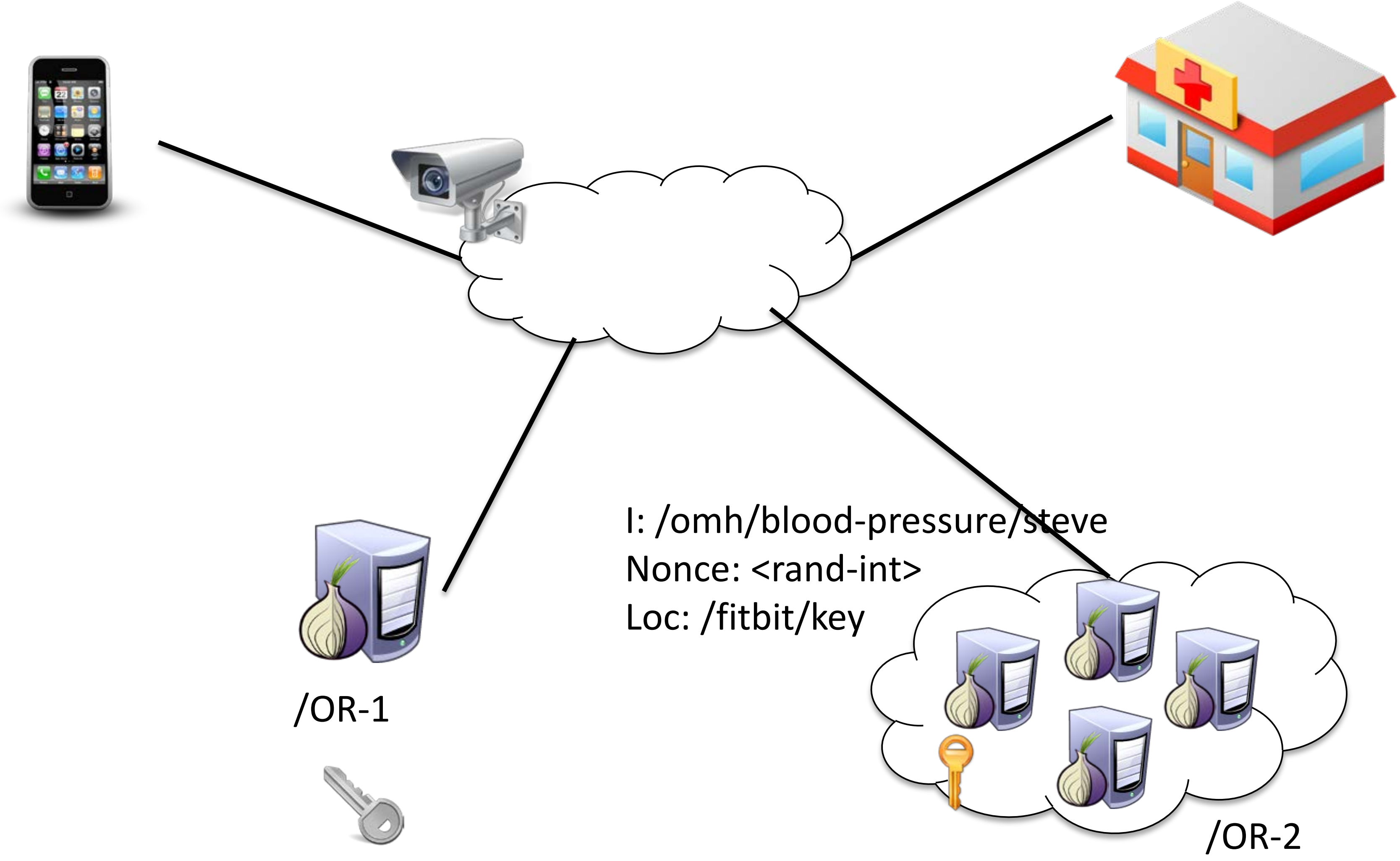
Onion Routing in NDN



I: /OR-2

I: /omh/blood-pressure/steve
Nonce: <rand-int>
Loc: /fitbit/key

Onion Routing in NDN

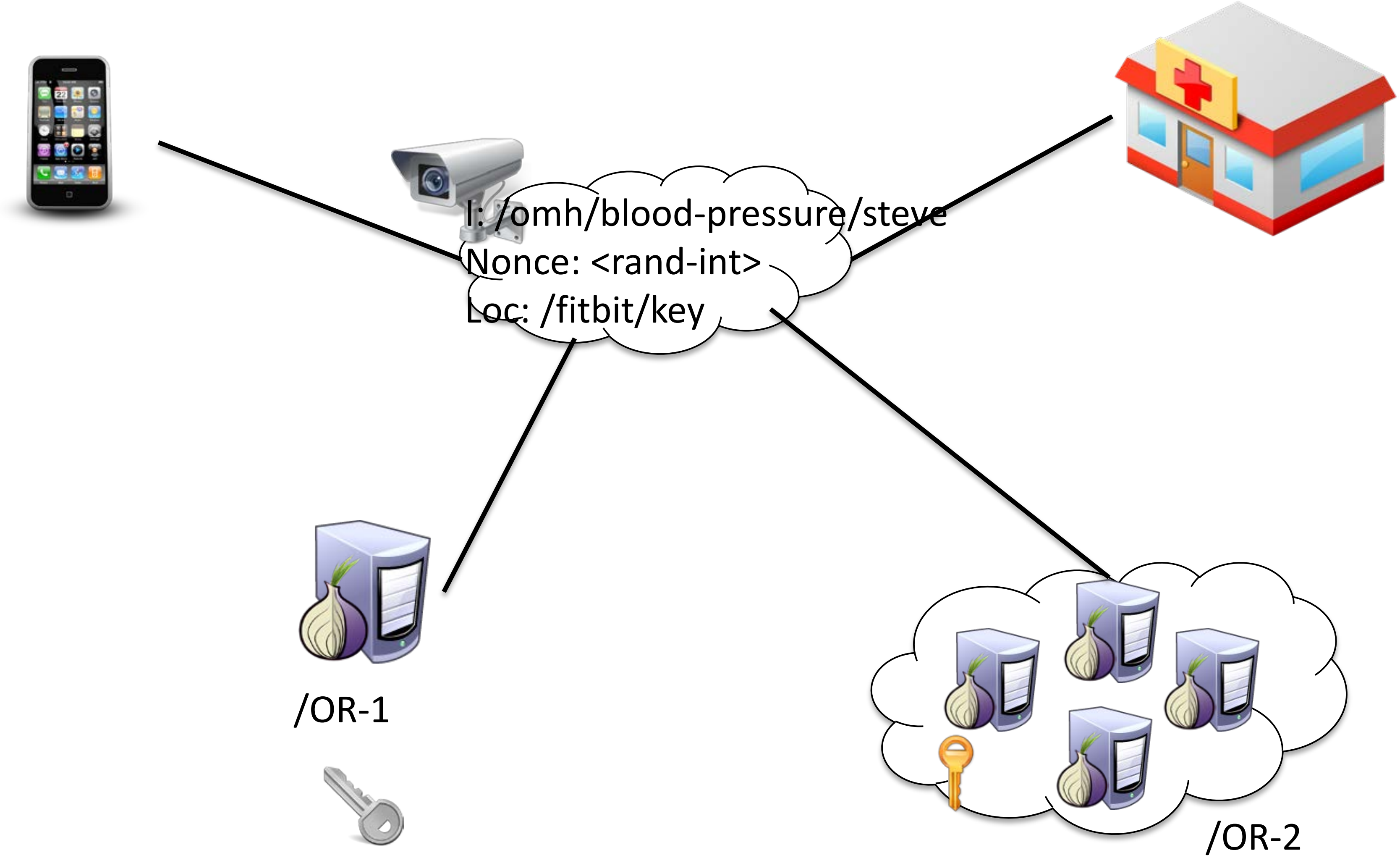


I: /omh/blood-pressure/steve
Nonce: <rand-int>
Loc: /fitbit/key

/OR-1

/OR-2

Onion Routing in NDN



I: /omh/blood-pressure/steve

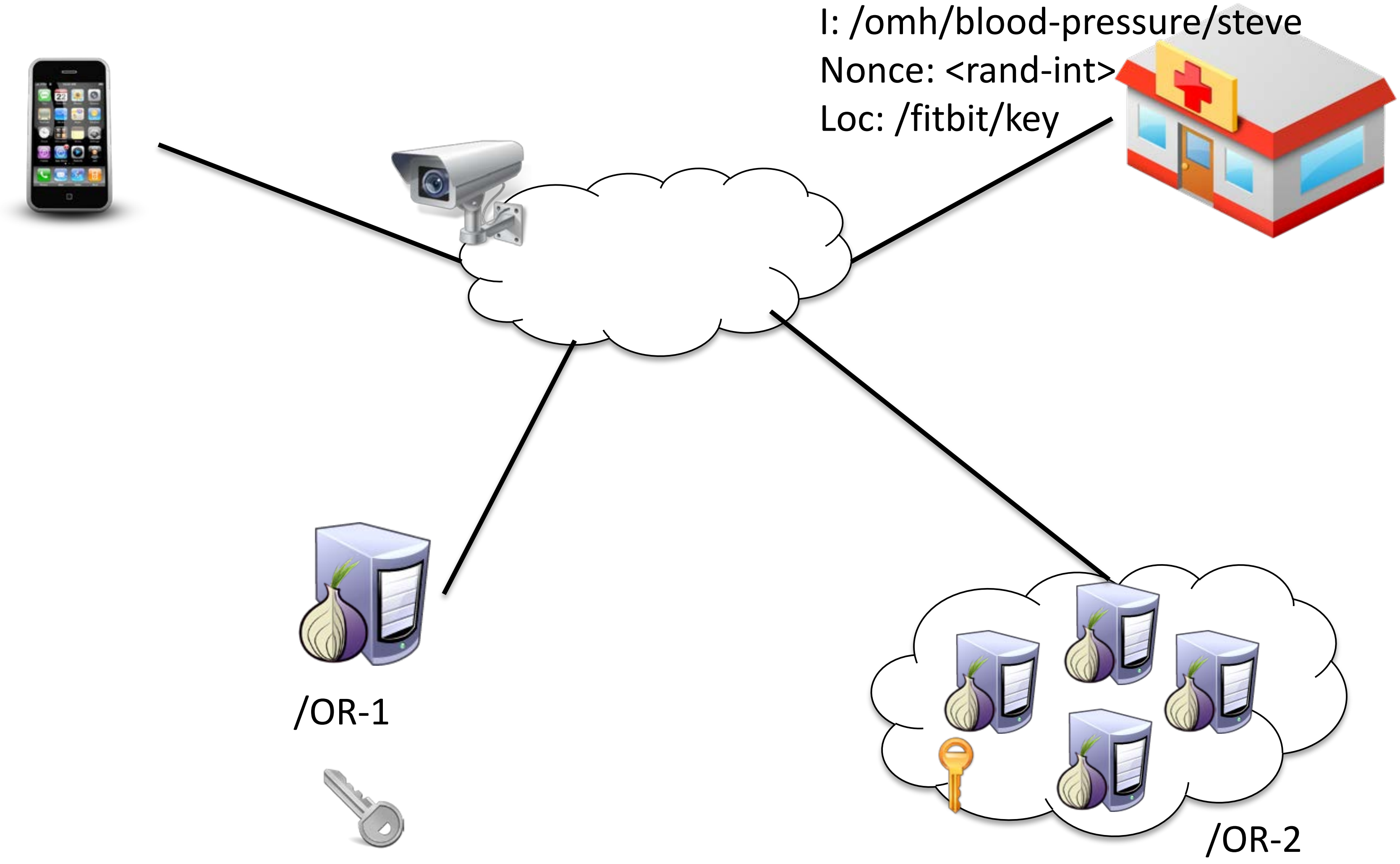
Nonce: <rand-int>

Loc: /fitbit/key

/OR-1

/OR-2

Onion Routing in NDN



I: /omh/blood-pressure/steve

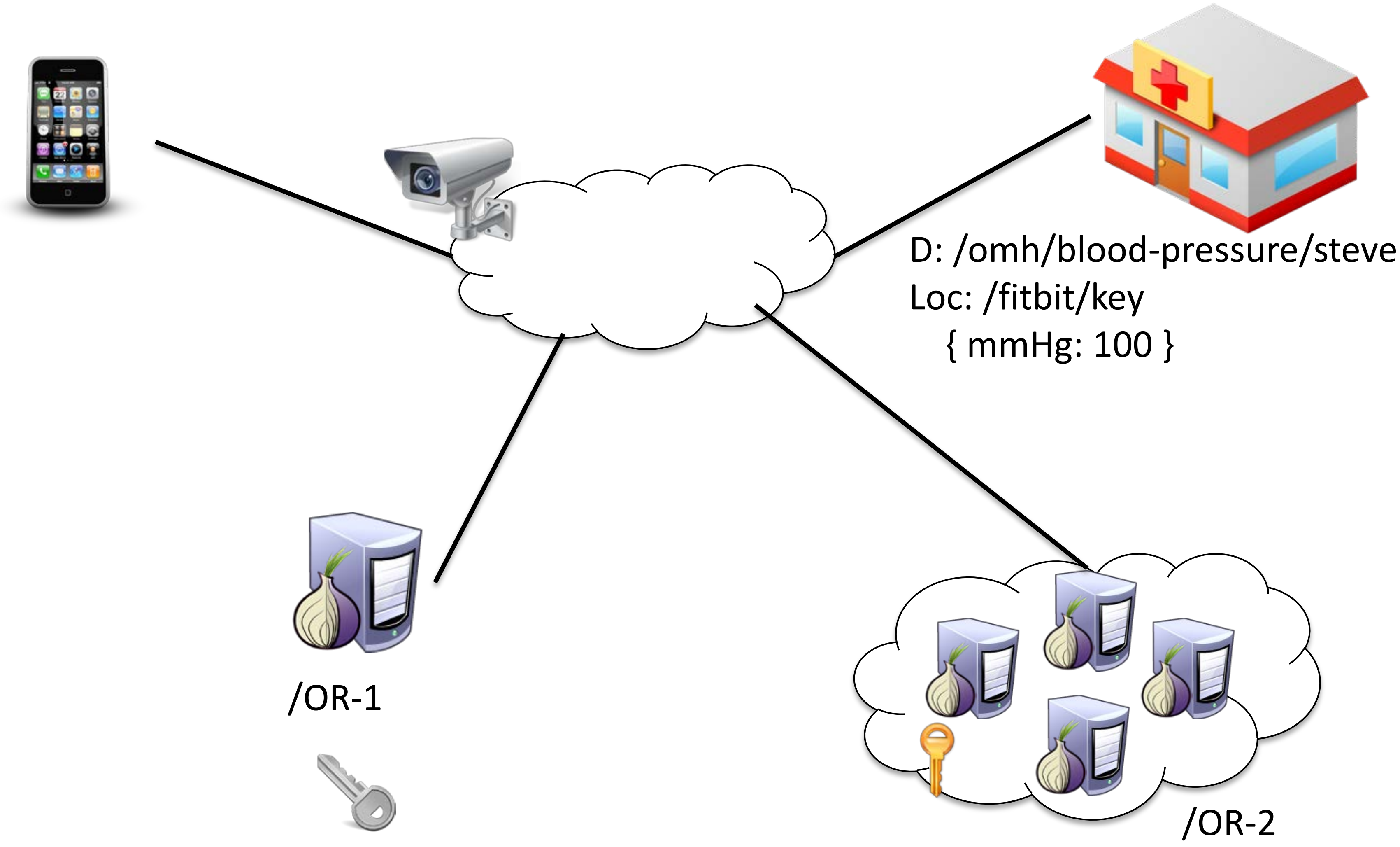
Nonce: <rand-int>

Loc: /fitbit/key

/OR-1

/OR-2

Onion Routing in NDN

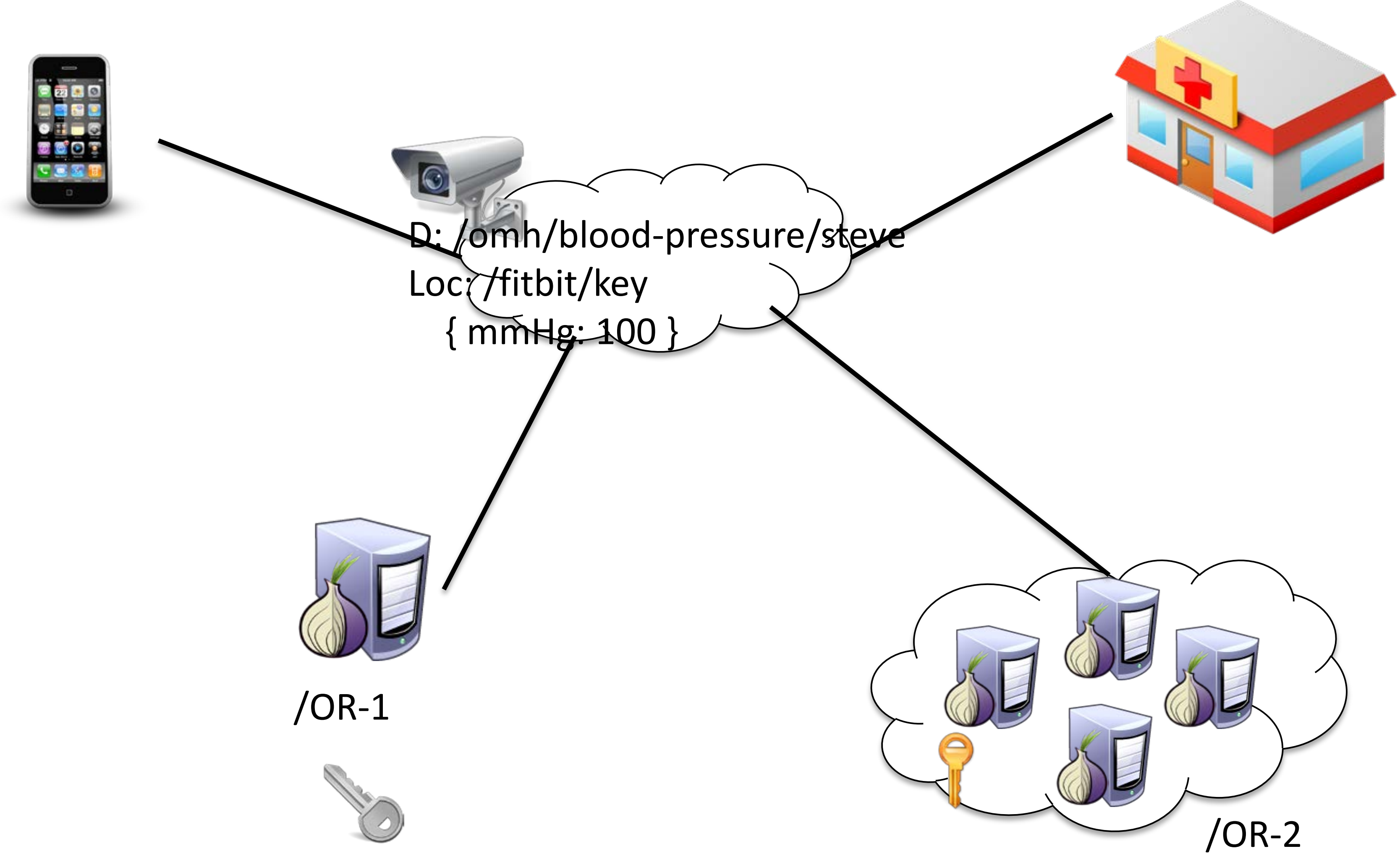


D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

/OR-1

/OR-2

Onion Routing in NDN

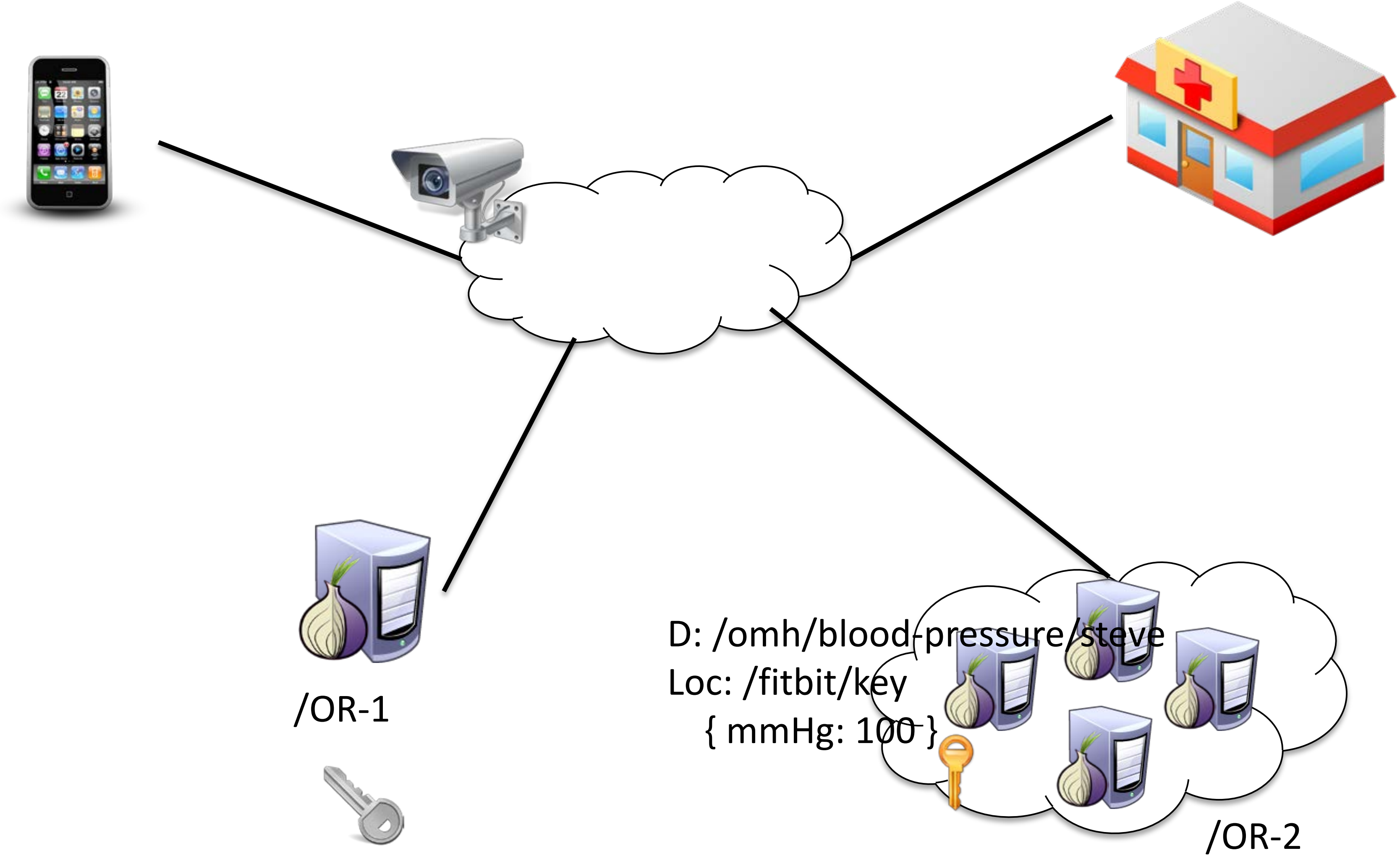


D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

/OR-1

/OR-2

Onion Routing in NDN

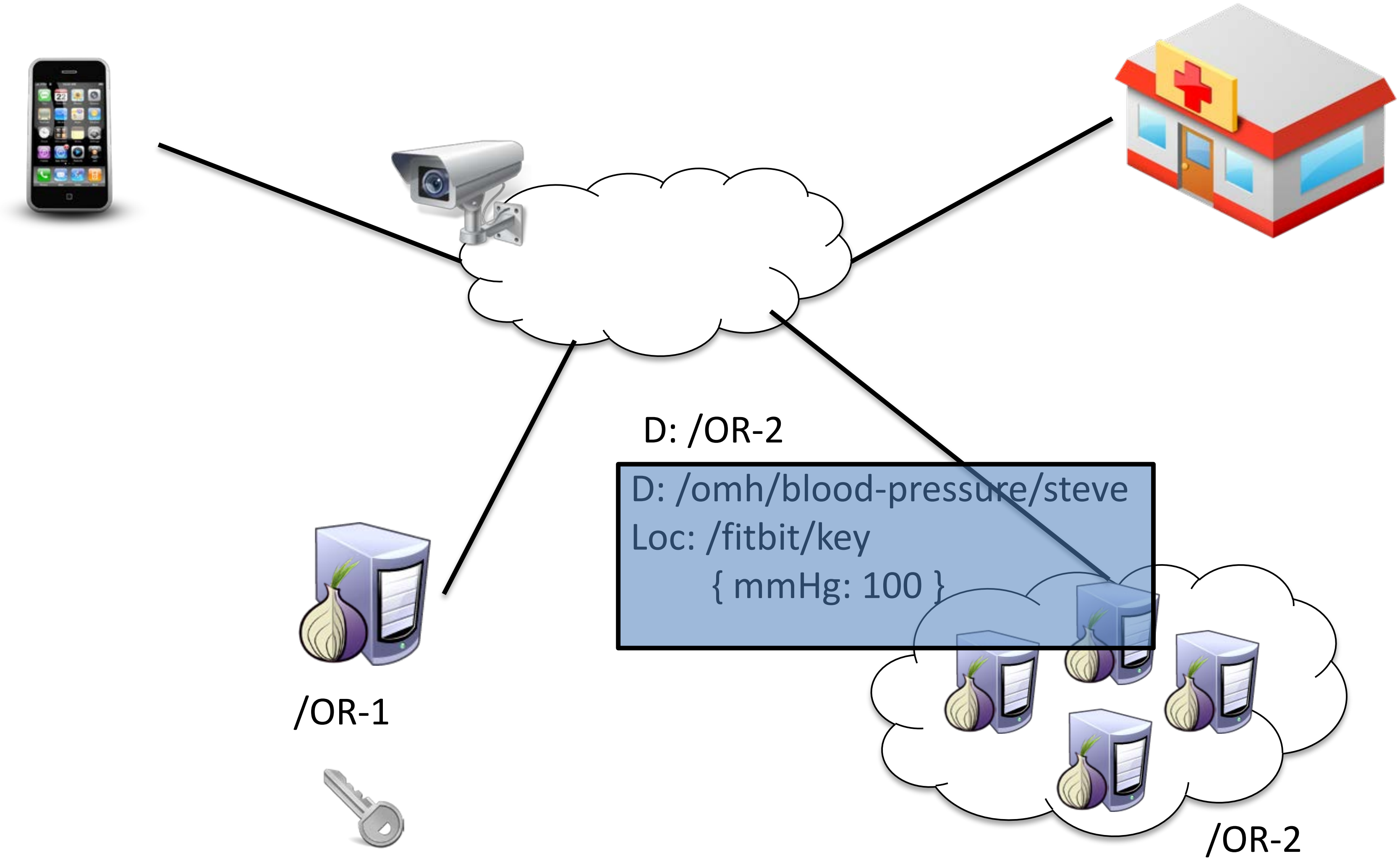


D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

/OR-1

/OR-2

Onion Routing in NDN



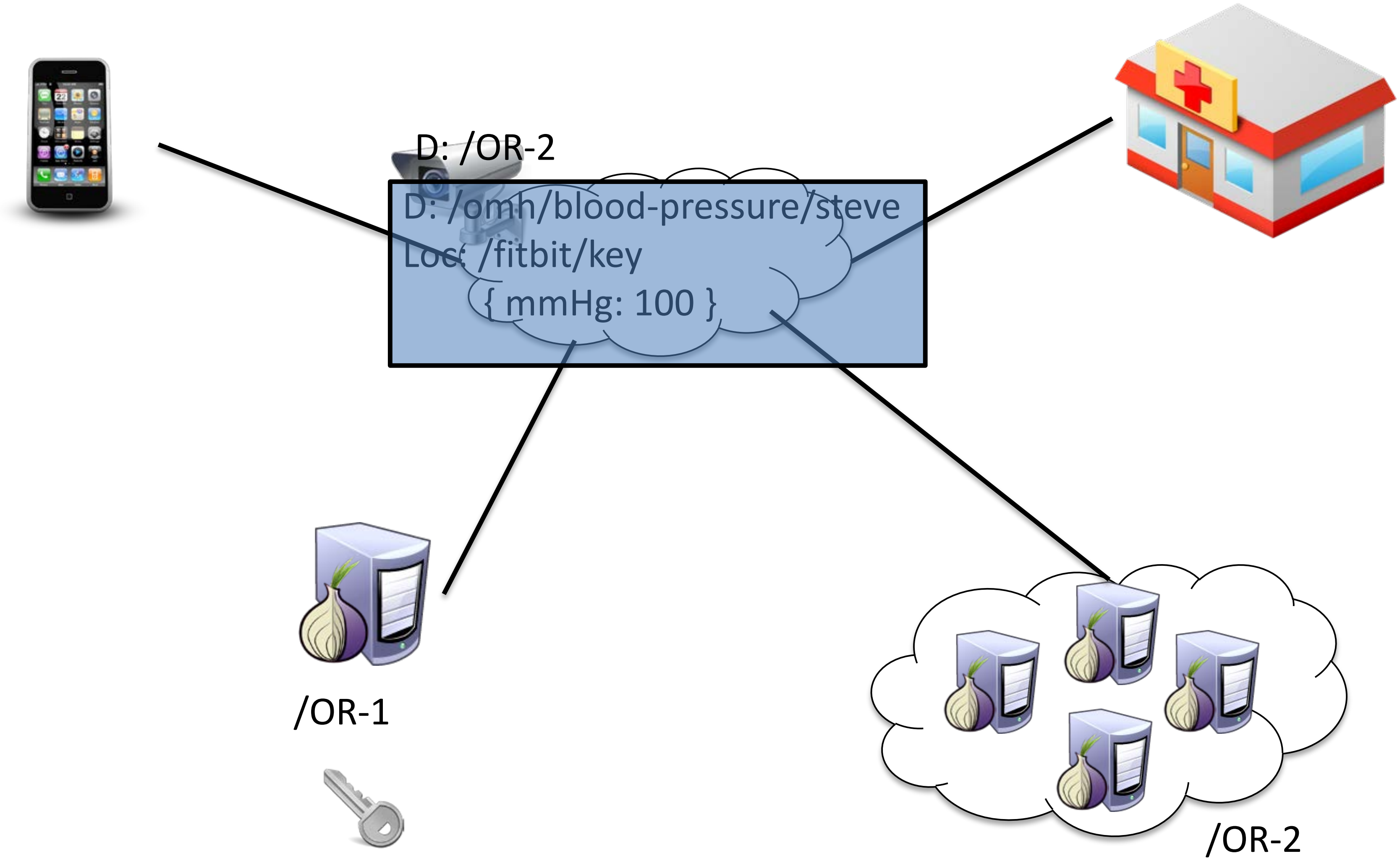
D: /OR-2

D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

/OR-1

/OR-2

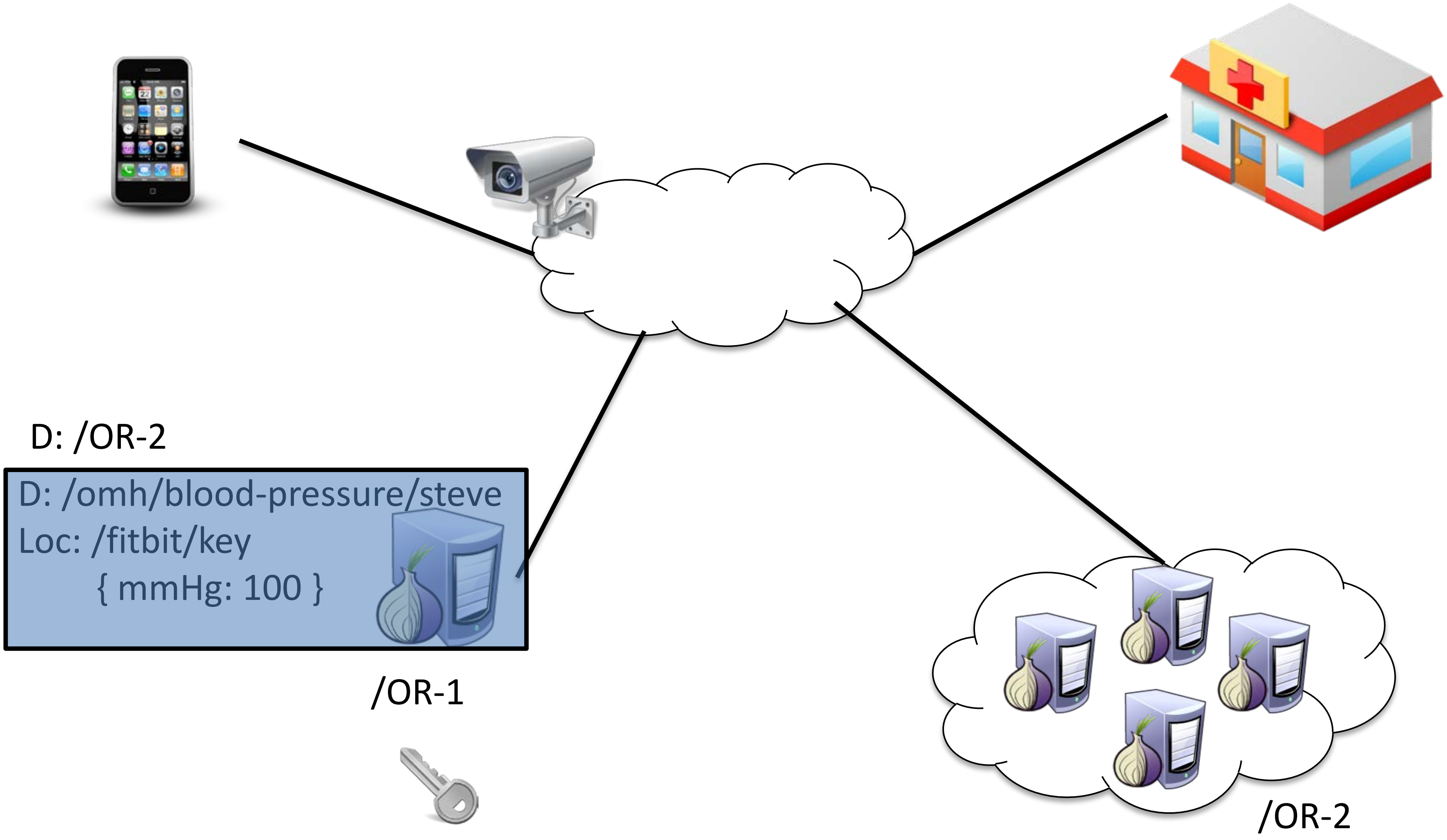
Onion Routing in NDN



D: /OR-2

D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

Onion Routing in NDN



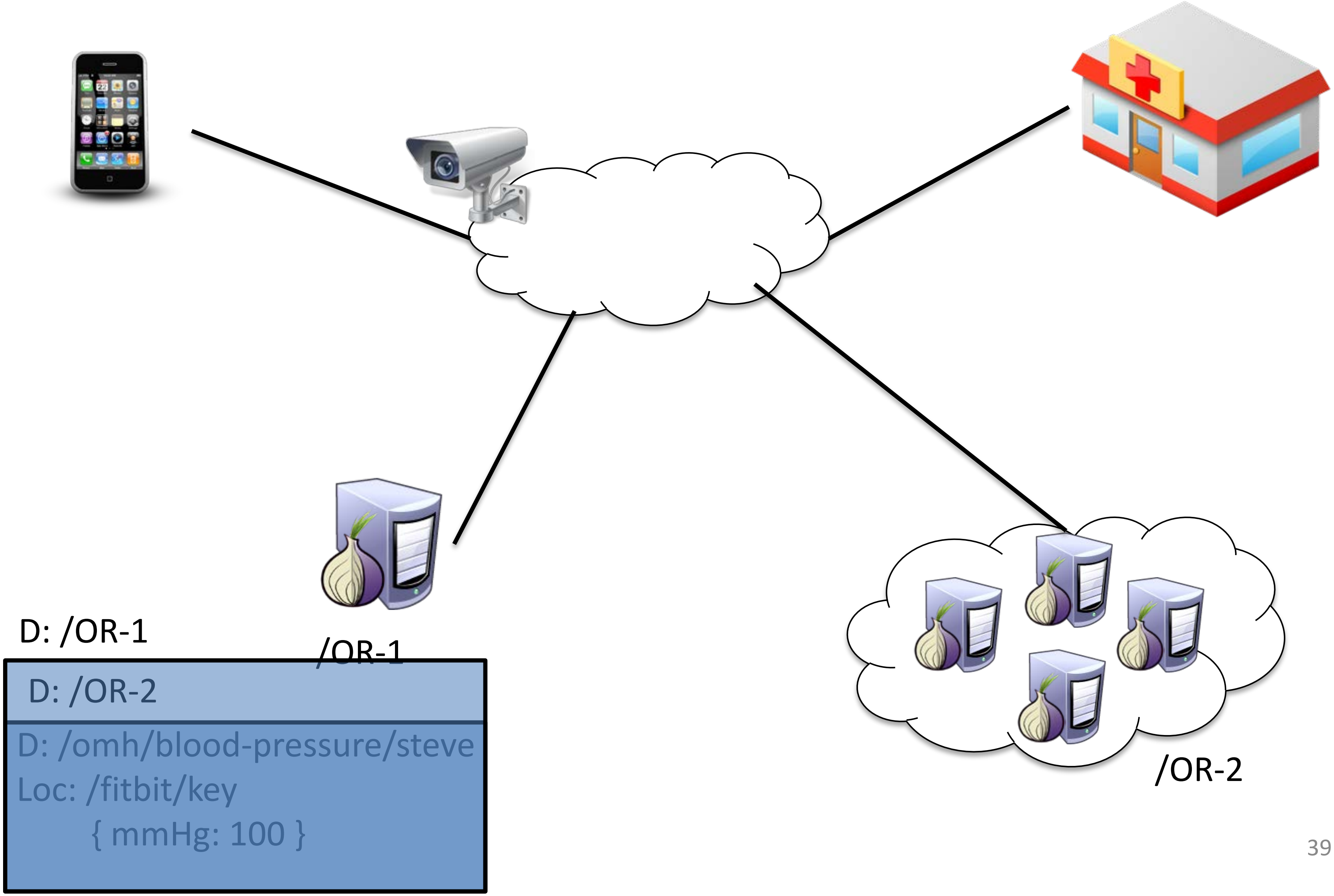
D: /OR-2

D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

/OR-1

/OR-2

Onion Routing in NDN

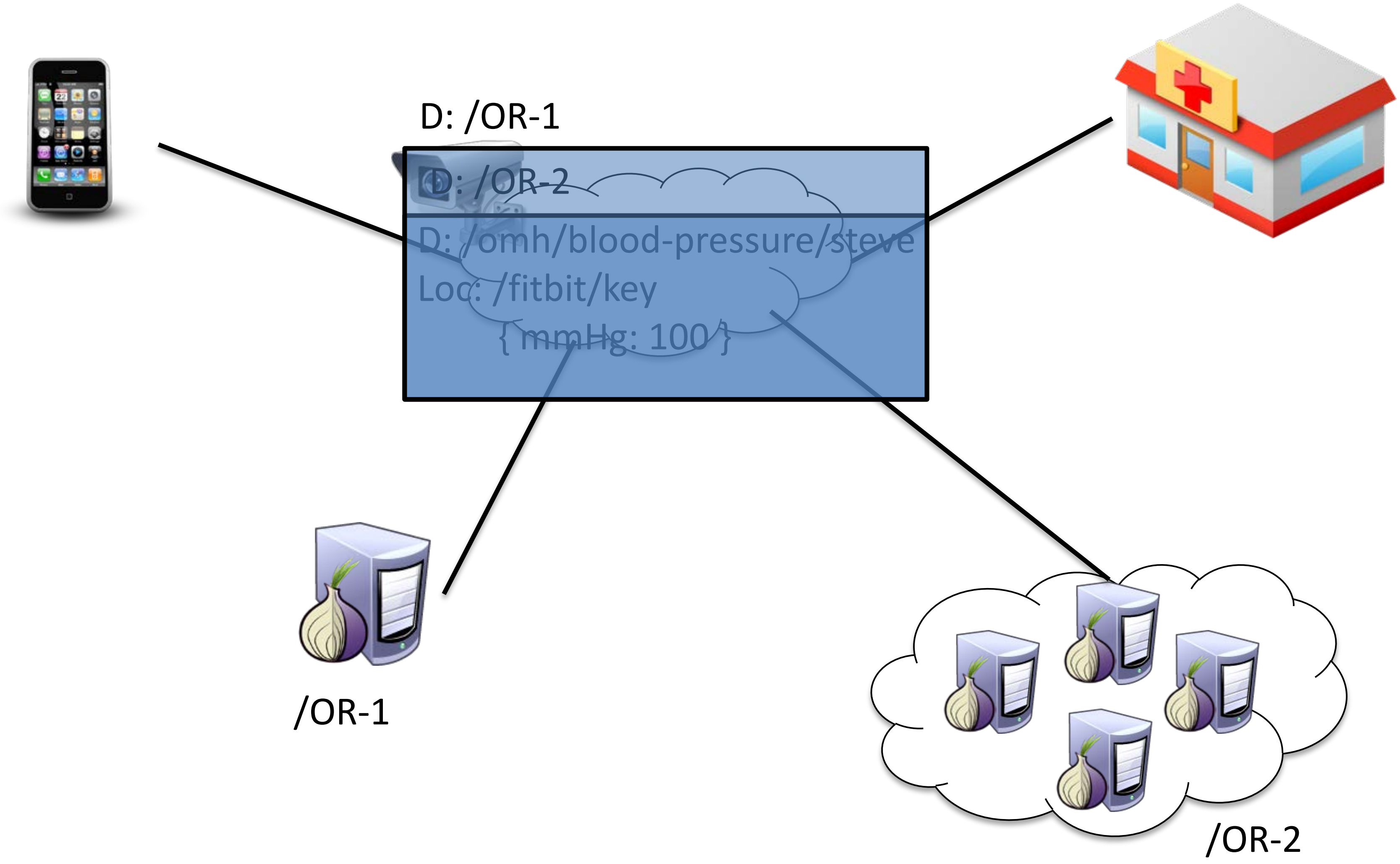


D: /OR-1

D: /OR-2

D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

Onion Routing in NDN



D: /OR-1

D: /OR-2

D: /omh/blood-pressure/steve

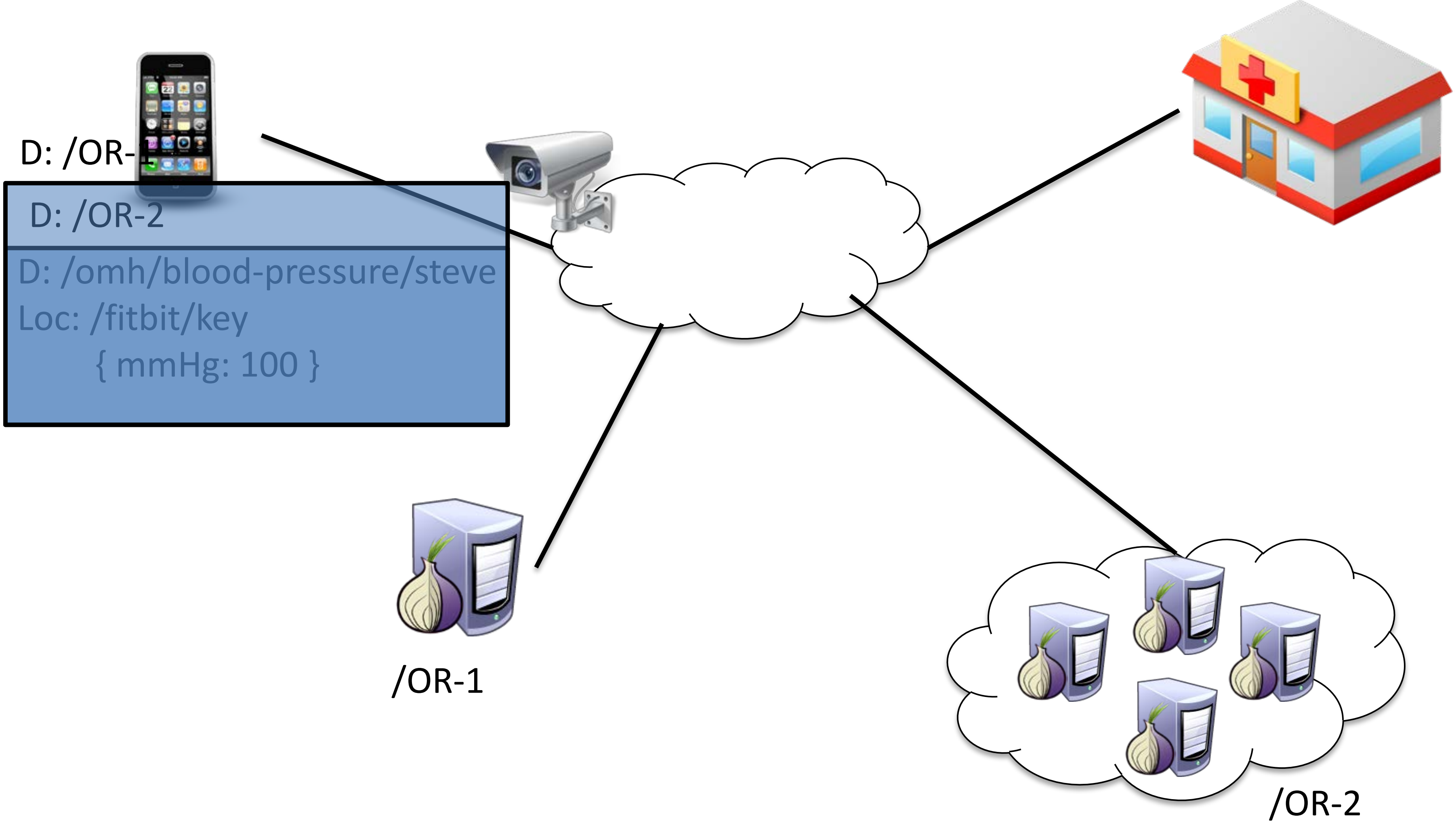
Loc: /fitbit/key

{ mmHg: 100 }

/OR-1

/OR-2

Onion Routing in NDN



D: /OR-1

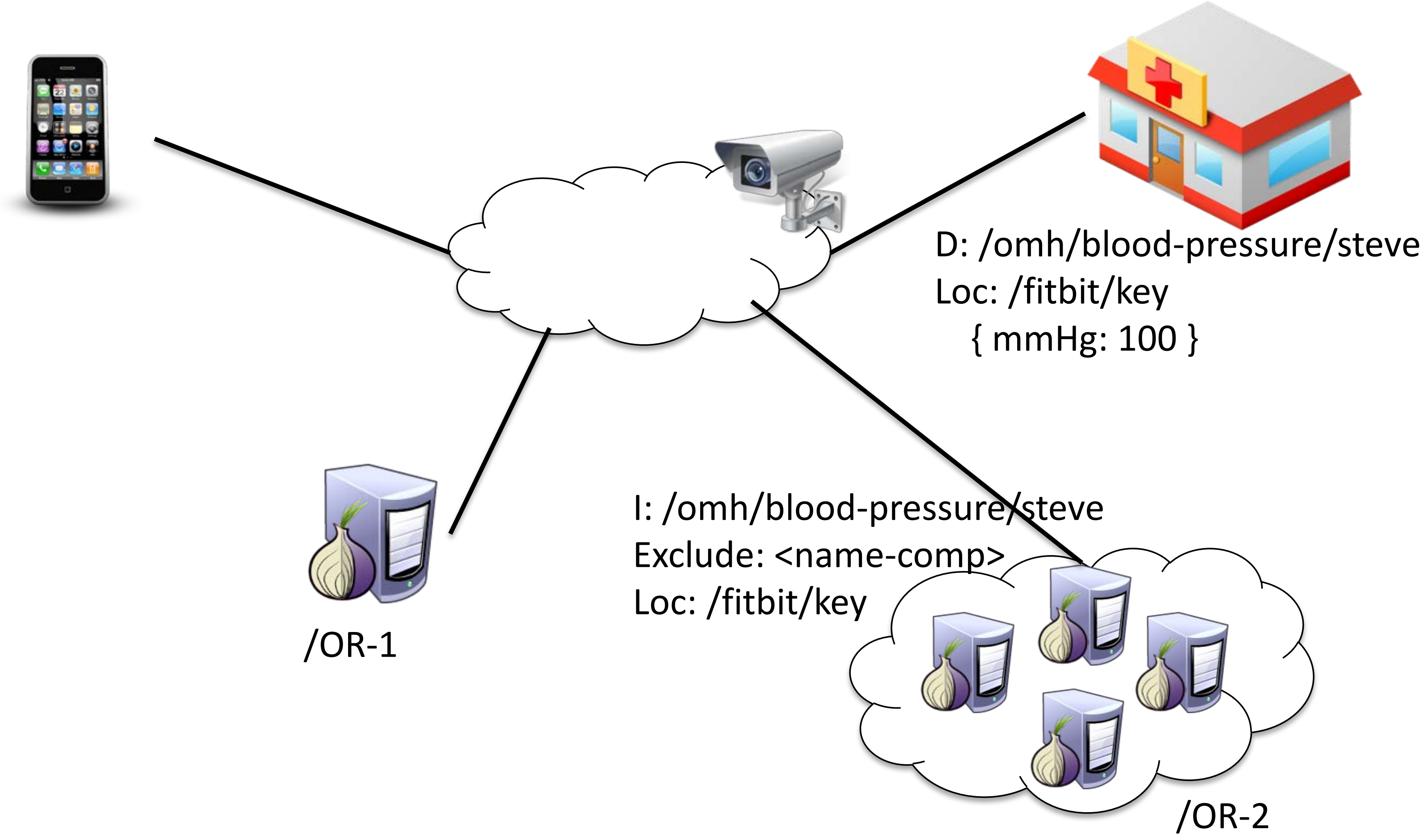
D: /OR-2

D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

Improvements Over Tor

- Need fewer relays than Tor (2 vs 3)
  - Potentially 1 less Internet-wide RTT
- ANDaNA paths are HIGHLY ephemeral
  - No path setup cost
  - Change keys and relays at will during a Data stream without interruption
  - Tor sets up much longer lived circuits in comparison (~ 10 minutes)
- Symmetric key session-based mode also available
  - Can be freely intermixed with public key crypto mode for the same Data stream.
- NDN gives us a lot for free
  - CS improves retransmission and chance for cache hit at exit node
  - OR prefixes can refer to multiple relays
  - OR directory more robust to attacks thanks to signed Data

The Exit Node Problem



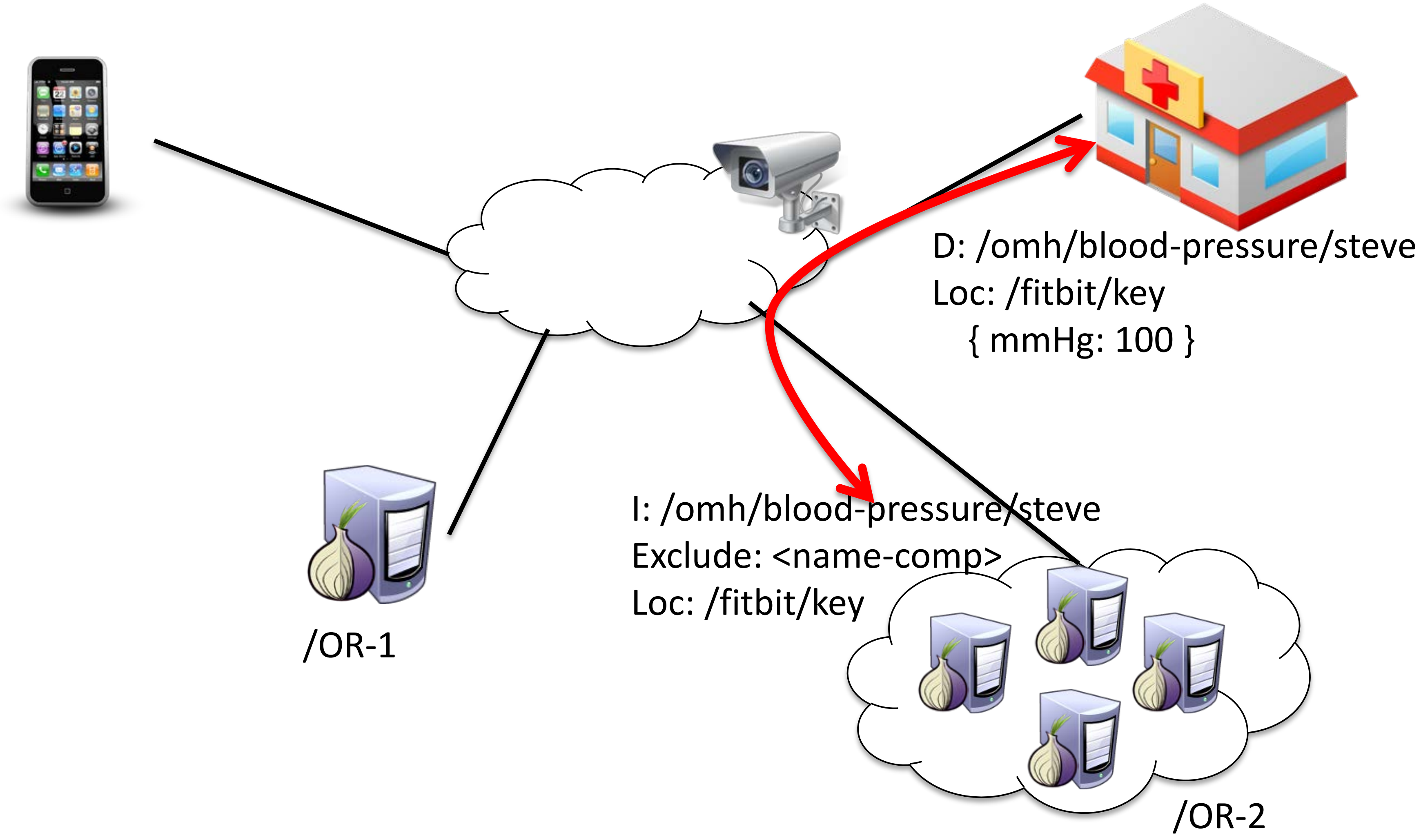
D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

I: /omh/blood-pressure/steve
Exclude: <name-comp>
Loc: /fitbit/key

/OR-1

/OR-2

The Exit Node Problem



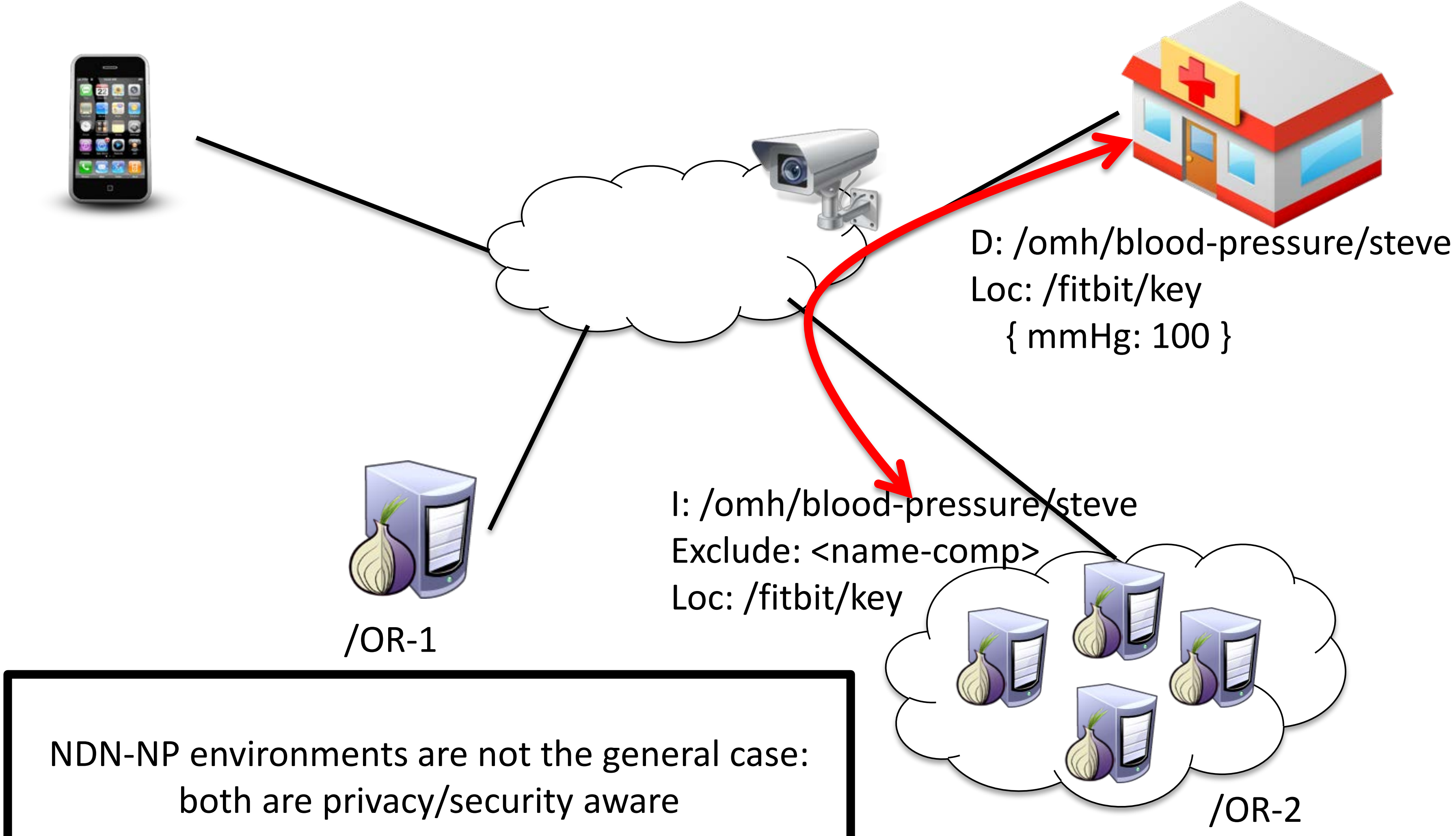
D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

I: /omh/blood-pressure/steve
Exclude: <name-comp>
Loc: /fitbit/key

/OR-1

/OR-2

The Exit Node Problem



D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

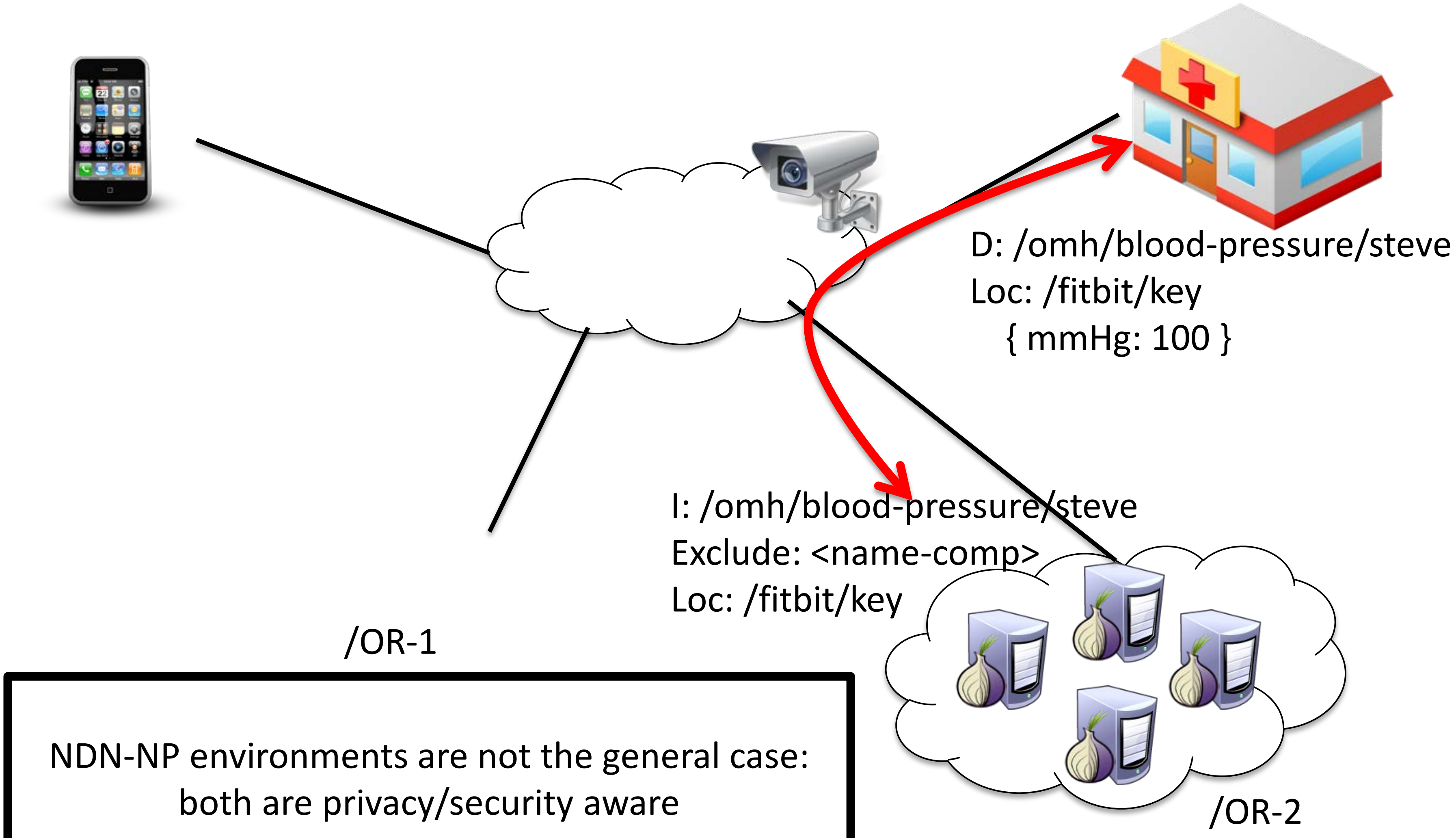
I: /omh/blood-pressure/steve
Exclude: <name-comp>
Loc: /fitbit/key

/OR-1

/OR-2

NDN-NP environments are not the general case:
both are privacy/security aware

The Exit Node Problem



D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

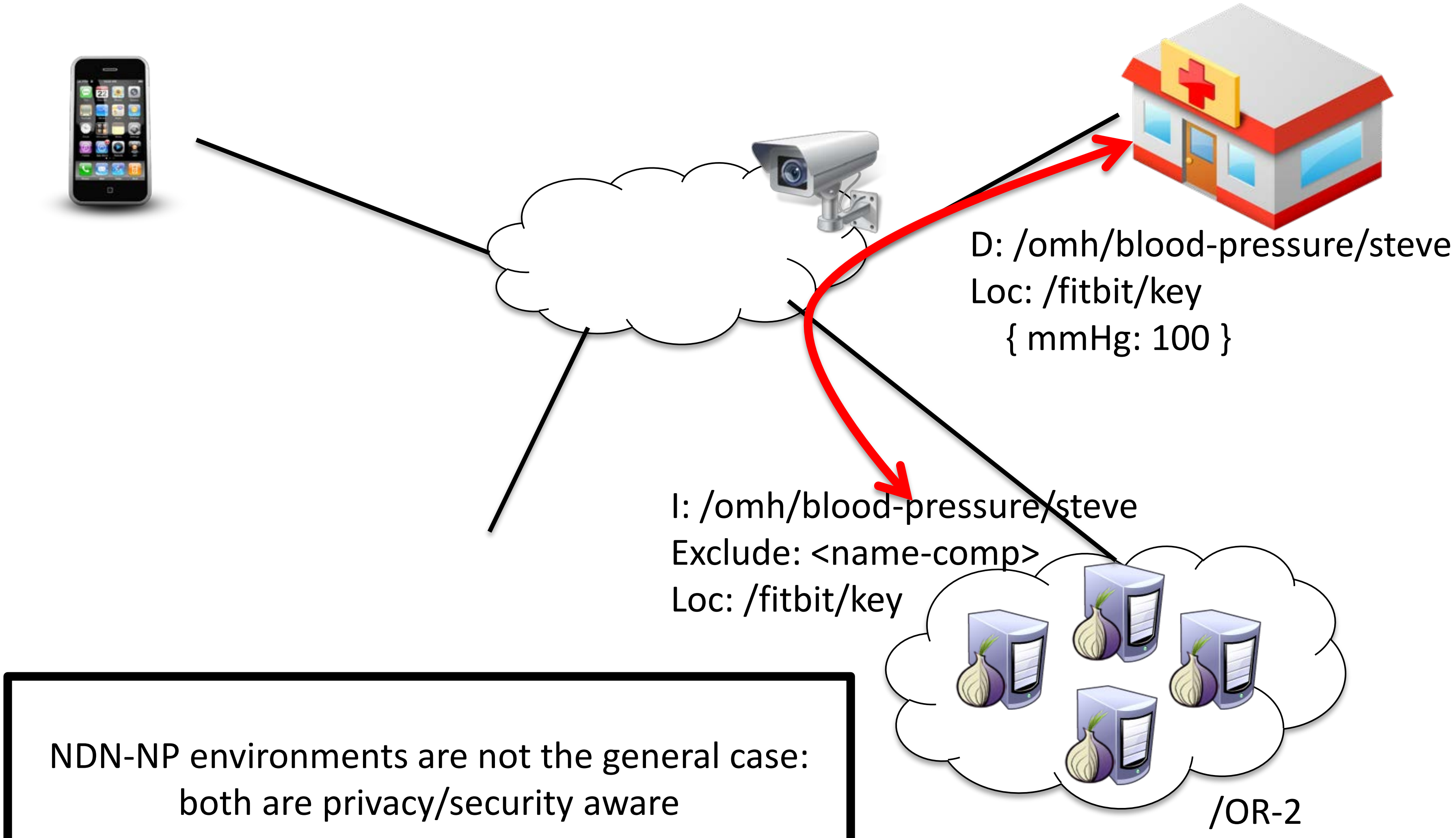
I: /omh/blood-pressure/steve
Exclude: <name-comp>
Loc: /fitbit/key

/OR-1

/OR-2

NDN-NP environments are not the general case: both are privacy/security aware

The Exit Node Problem



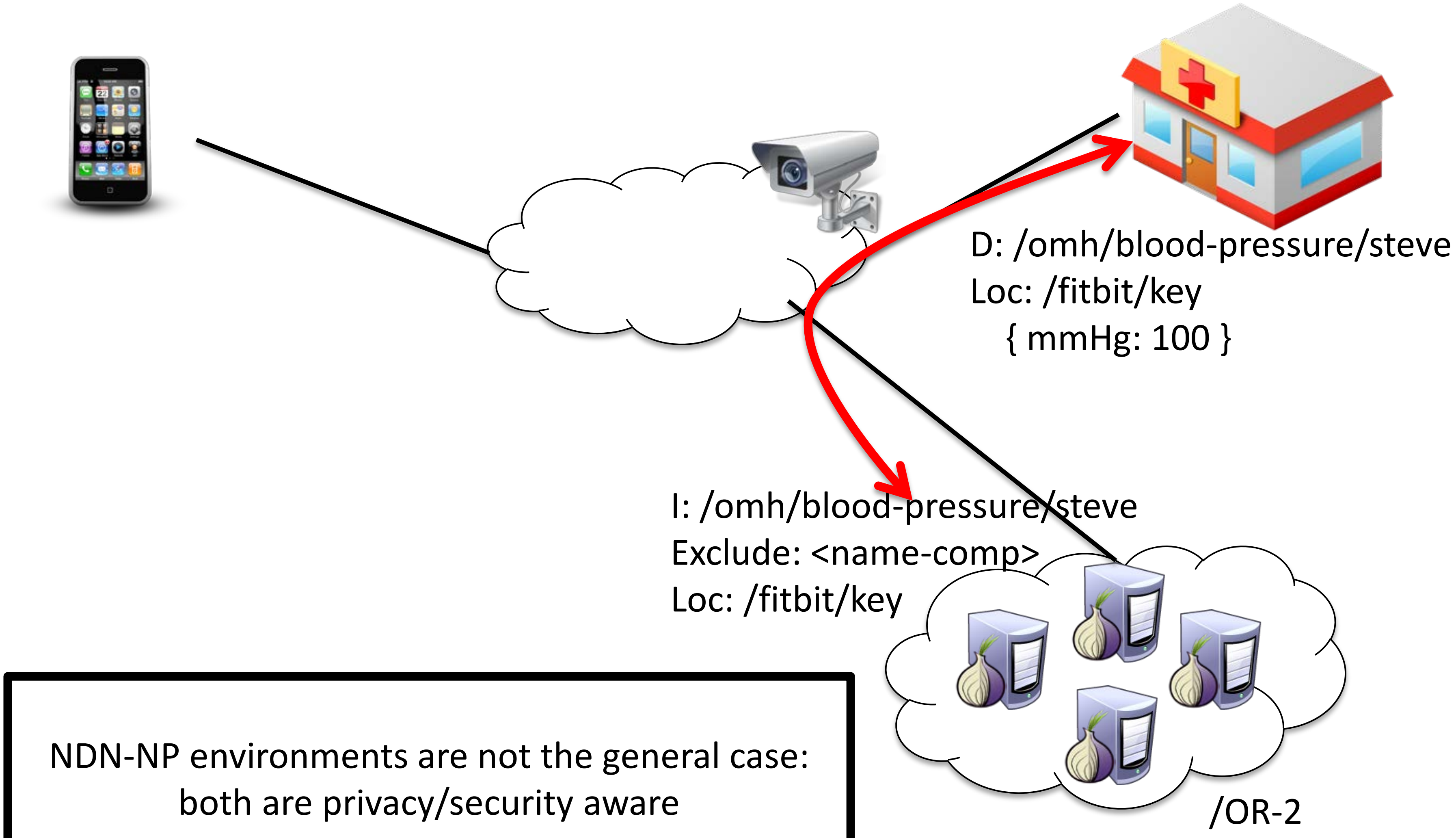
D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

I: /omh/blood-pressure/steve
Exclude: <name-comp>
Loc: /fitbit/key

/OR-2

NDN-NP environments are not the general case: both are privacy/security aware

The Exit Node Problem



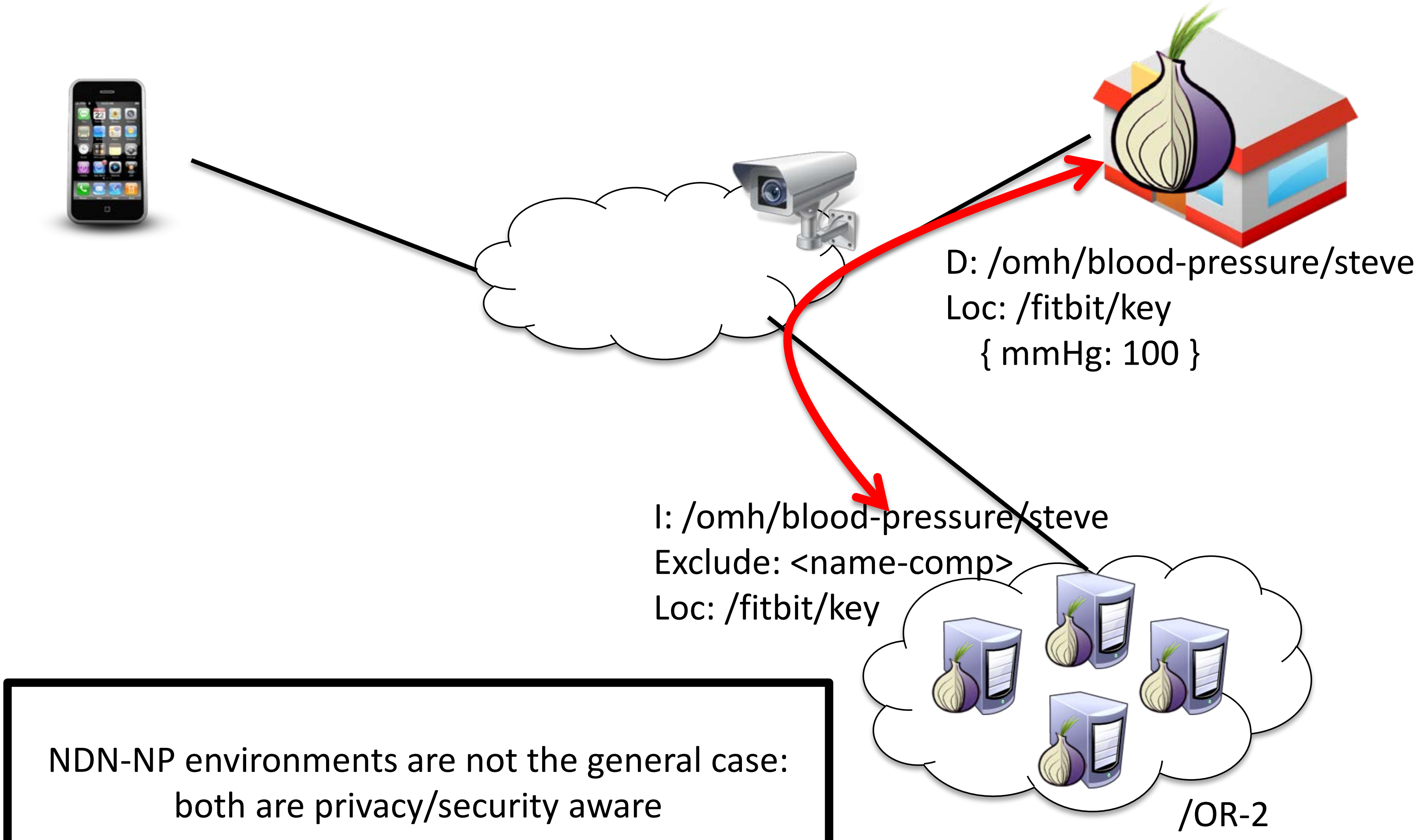
D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

I: /omh/blood-pressure/steve
Exclude: <name-comp>
Loc: /fitbit/key

/OR-2

NDN-NP environments are not the general case:
both are privacy/security aware

The Exit Node Problem



D: /omh/blood-pressure/steve
Loc: /fitbit/key
{ mmHg: 100 }

I: /omh/blood-pressure/steve
Exclude: <name-comp>
Loc: /fitbit/key

/OR-2

NDN-NP environments are not the general case:
both are privacy/security aware

Summary

- ANDaNA provides a Tor-like service for NDN, but new tradeoffs to consider

- ANDaNA is fundamentally a proxy: use as many (or few) relays as needed

Thoughts

- What’s the threat model for NDN-NP?
- Tradeoffs:
  - ANDaNA provides low latency anonymity
  - Mix networks could be used if NDN-NP can tolerate latency
- Implementing confidentiality:
  - Confidentially must be left to applications.
  - Users don’t own the network, but can own overlays