Interoperable Digital Proximity Tracing (IDPT) protocol

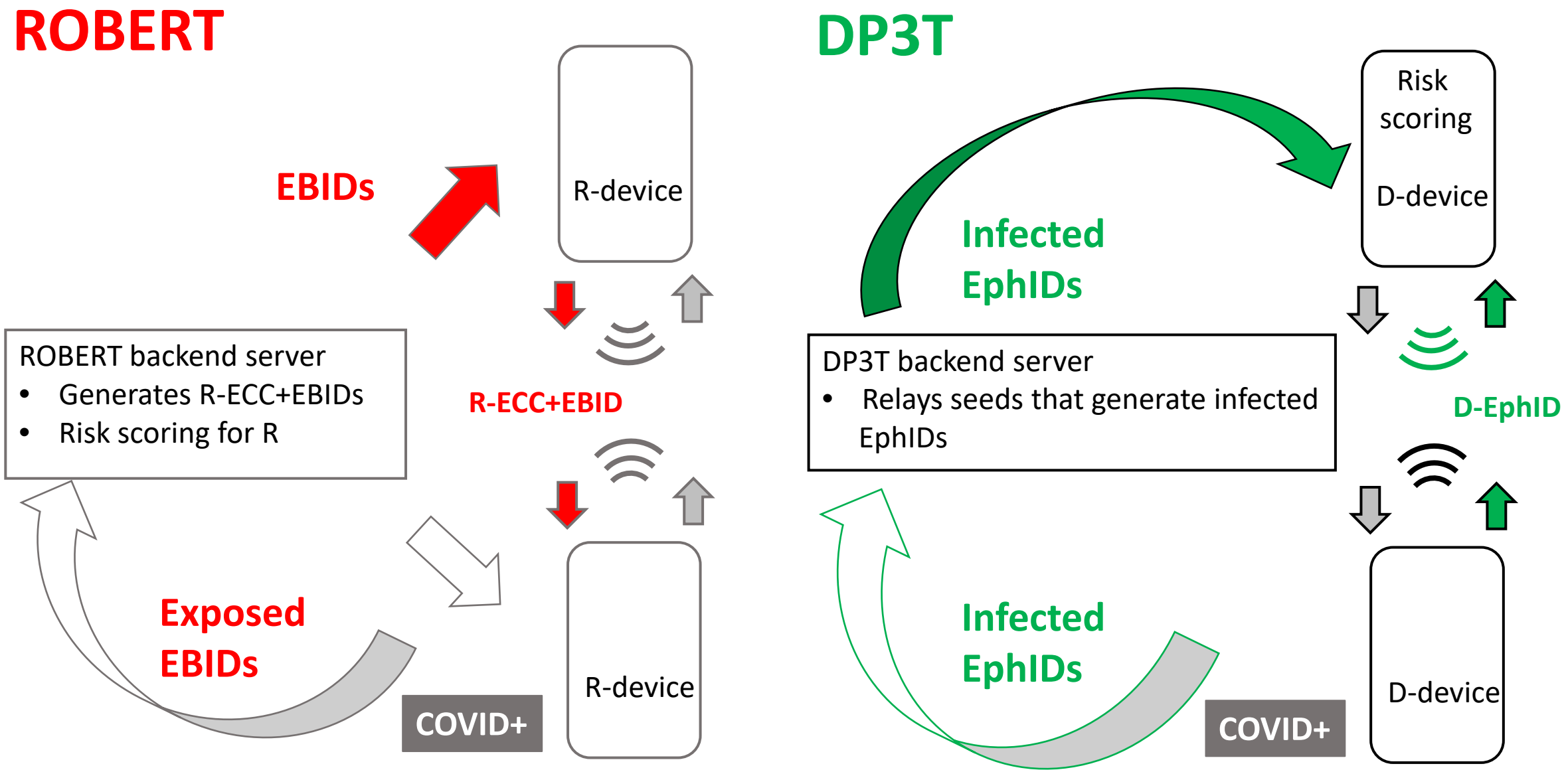
Jorge García-Vidal UPC, BSC-CNS
Secretaría de Estado de Digitalización e Inteligencia Artificial
Ministerio de Asuntos Económicos y Transformación Digital

eHealth Network meeting, June 10th 2020

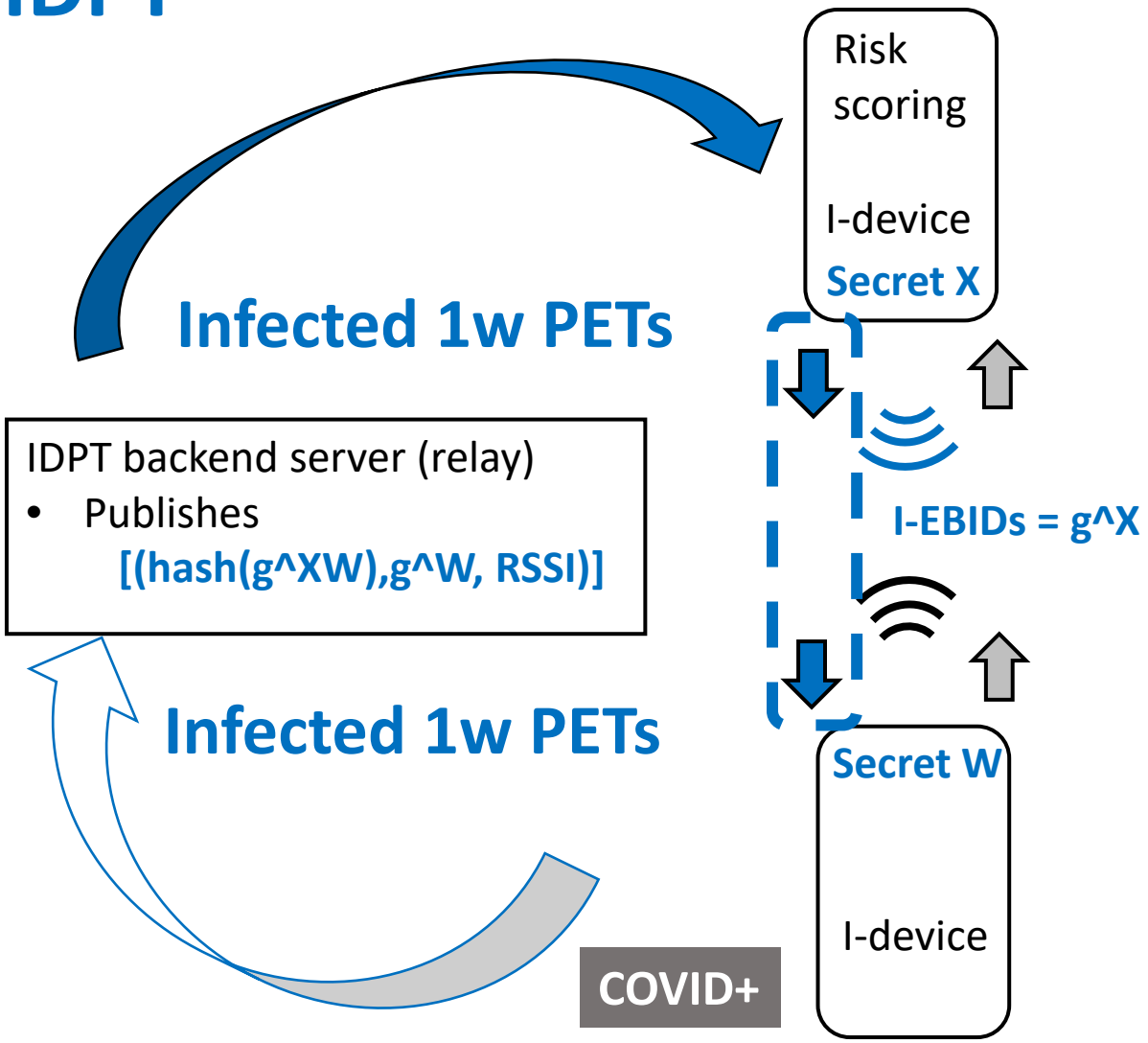
Interoperability of ROBERT and DP3T+IDPT

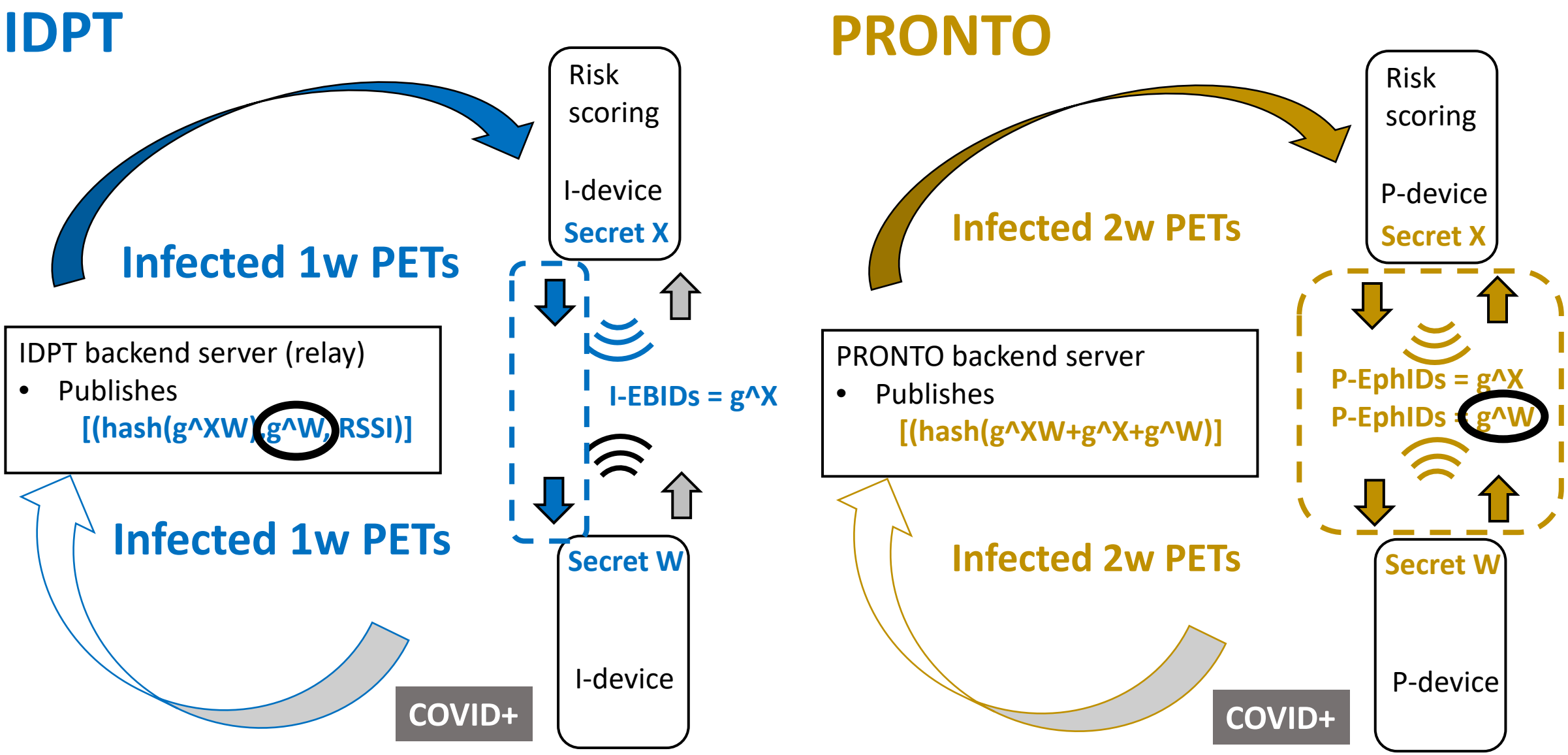
Assume that in the same geographic area we have users of 3 different types of digital proximity tracing applications:

- Applications R (ROBERT), D (DP3T), and I (DP3T + IDPT)
- Assume that applications I and D interoperate.
- We achieve interoperability between the I and R, meaning that **if a user of the application R/I reports COVID+, devices of users of the application I/R who were exposed will be also notified**.
- **The privacy properties of the 3 apps do not change.**

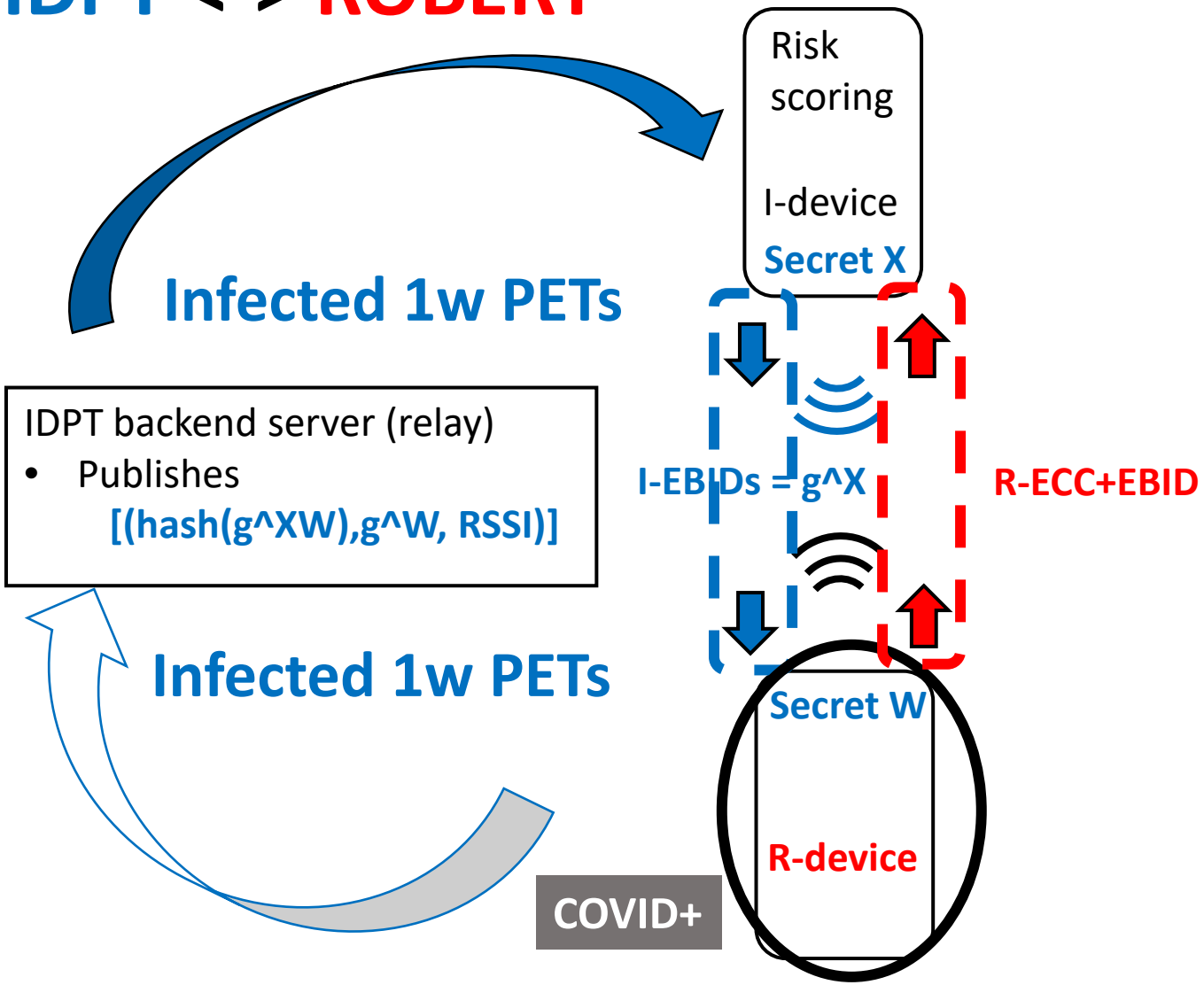

ROBERT
EBIDs
R-device
ROBERT backend server
• Generates R-ECC+EBIDs
• Risk scoring for R
R-ECC+EBID
Exposed
EBIDs
COVID+
R-device
DP3T
Risk
scoring
D-device
Infected
EphIDs
DP3T backend server
• Relays seeds that generate infected EphIDs
D-EphID
Infected
EphIDs
COVID+
D-device

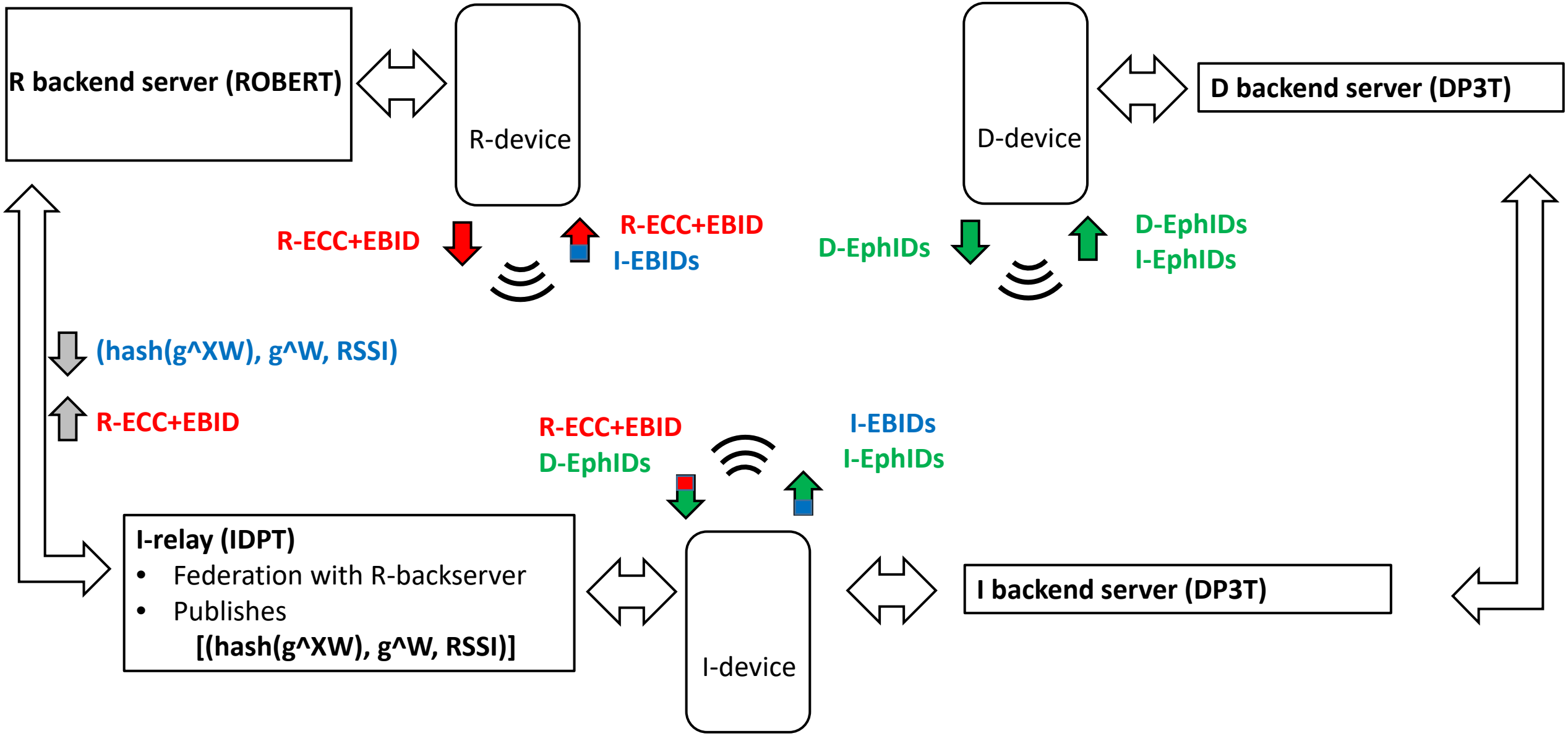
IDPT

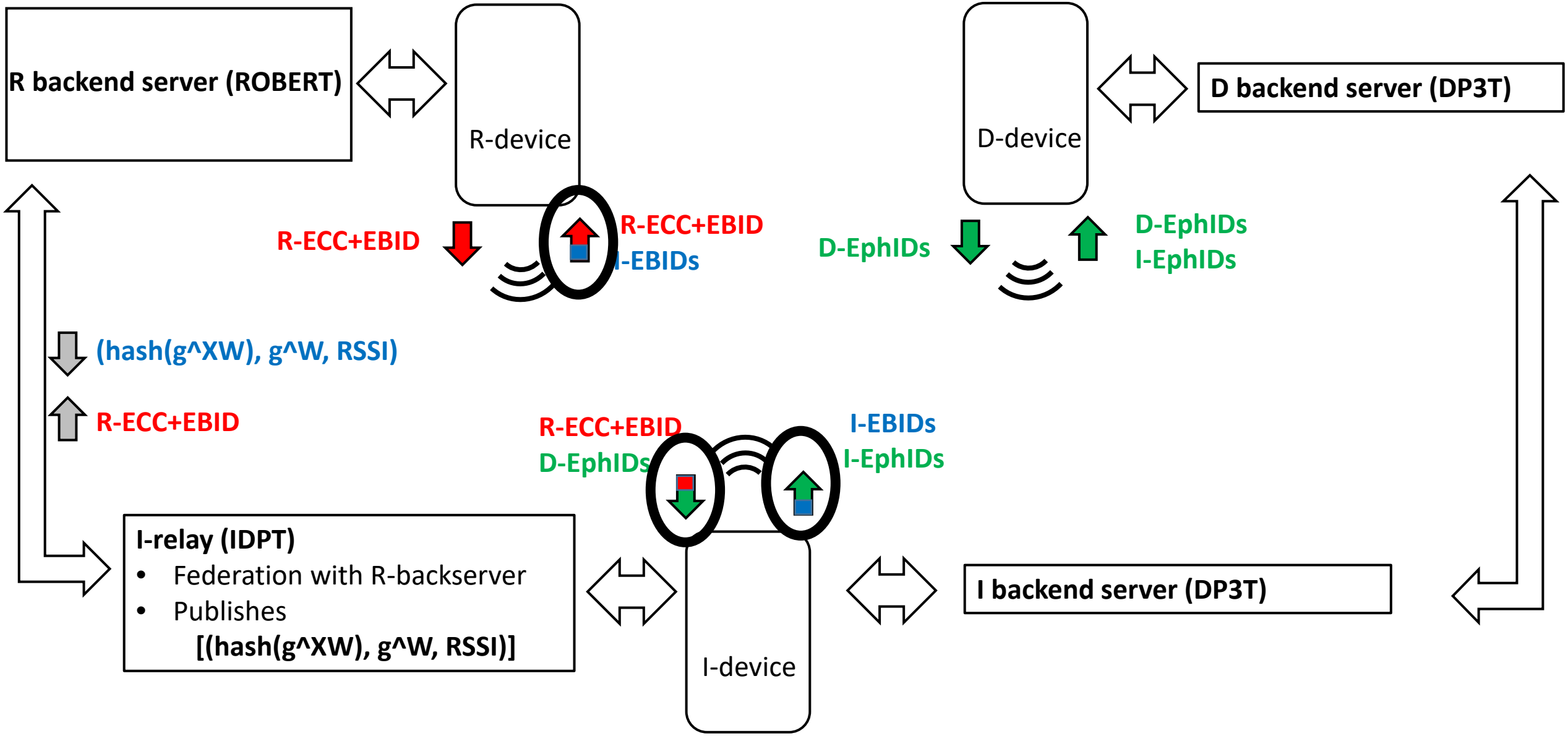


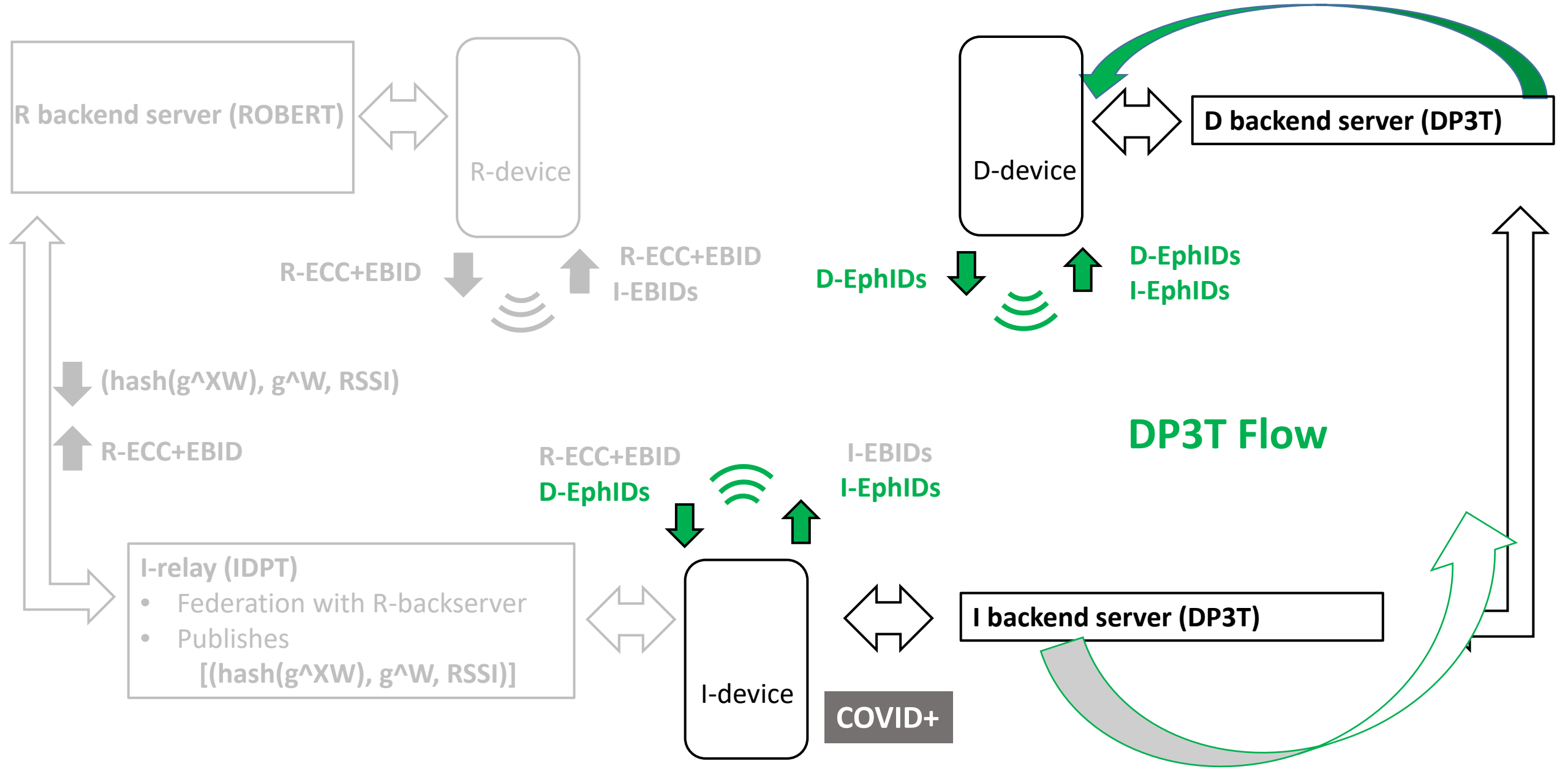

IDPT
Risk scoring
I-device
Secret X
Infected 1w PETs
IDPT backend server (relay)
• Publishes
[(hash(g^XW), g^W, RSSI)]
I-EBIDs = g^X
Infected 1w PETs
Secret W
I-device
COVID+
PRONTO
Risk scoring
P-device
Secret X
Infected 2w PETs
PRONTO backend server
• Publishes
[(hash(g^XW+g^X+g^W)]
P-EphIDs = g^X
P-EphIDs = g^W
Infected 2w PETs
Secret W
P-device
COVID+

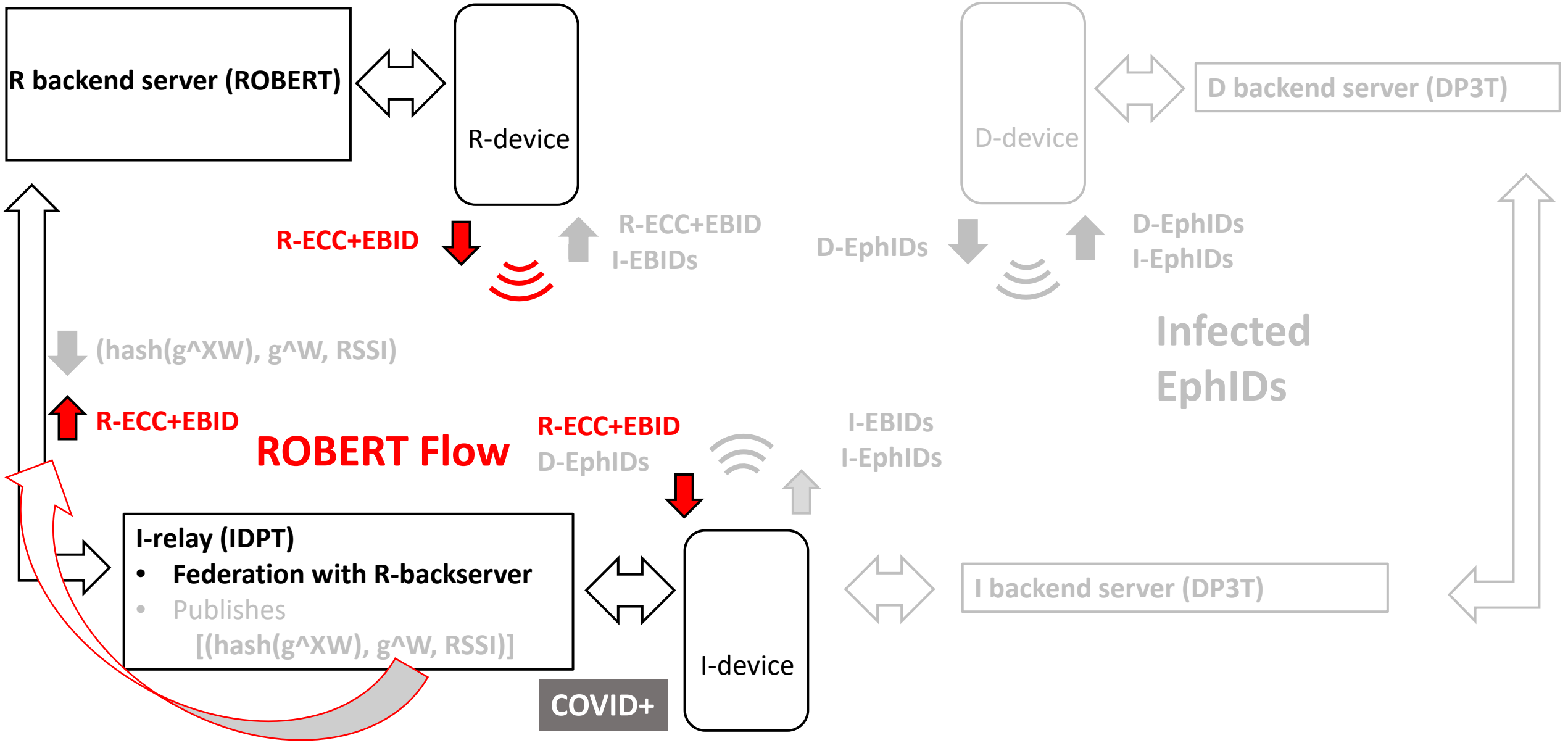
IDPT <-> ROBERT

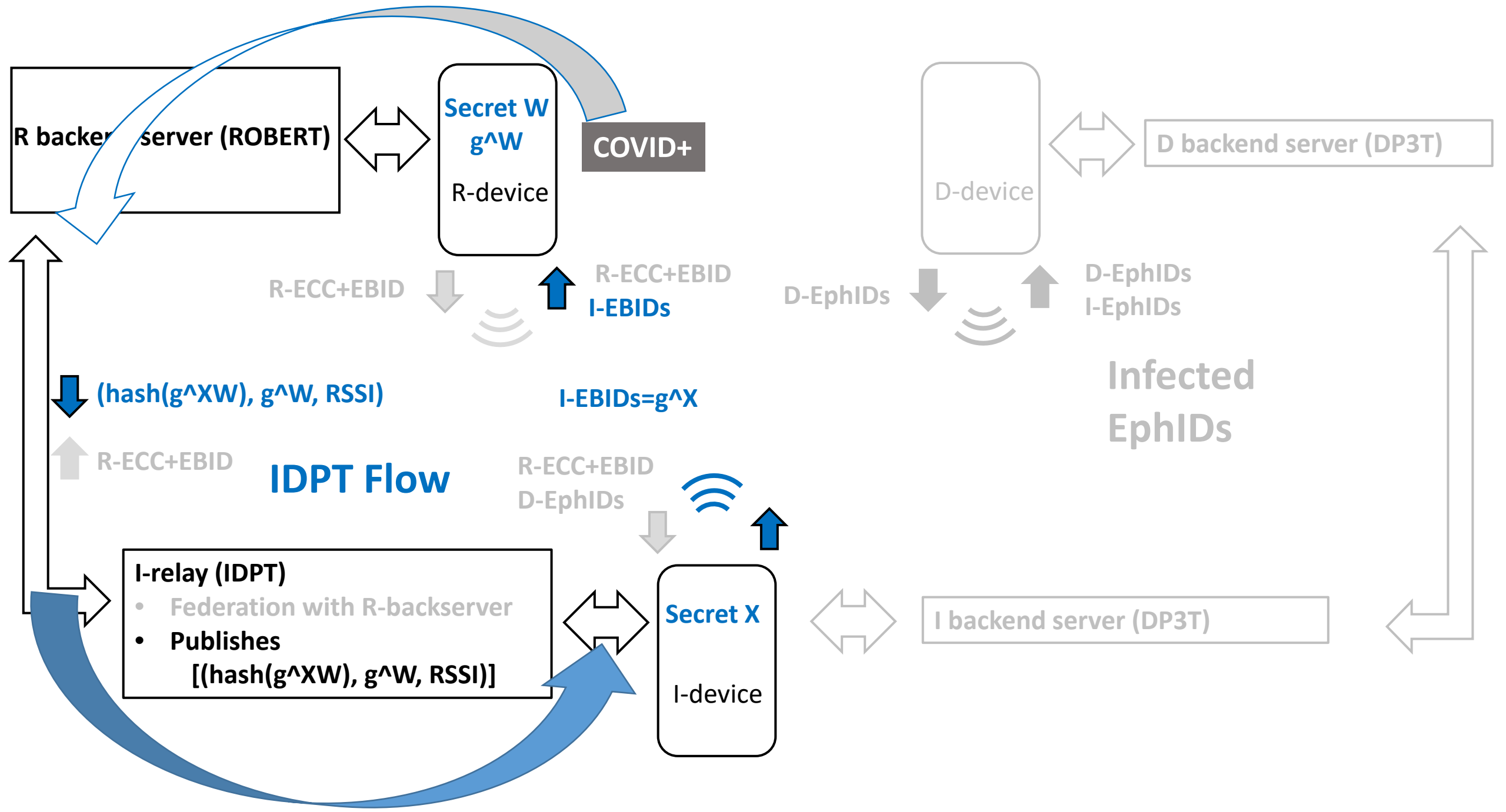



R backend server (ROBERT)
R-device
D-device
D backend server (DP3T)
R-ECC+EBID
R-ECC+EBID
I-EBIDs
D-EphIDs
D-EphIDs
I-EphIDs
(hash(g^XW), g^W, RSSI)
R-ECC+EBID
R-ECC+EBID
D-EphIDs
I-EBIDs
I-EphIDs
I-relay (IDPT)
• Federation with R-backserver
• Publishes
[(hash(g^XW), g^W, RSSI)]
I-device
I backend server (DP3T)


R backend server (ROBERT)
R-device
D-device
D backend server (DP3T)
R-ECC+EBID
R-ECC+EBID
I-EBIDs
D-EphIDs
D-EphIDs
I-EphIDs
(hash(g^XW), g^W, RSSI)
R-ECC+EBID
R-ECC+EBID
D-EphIDs
I-EBIDs
I-EphIDs
I-relay (IDPT)
• Federation with R-backserver
• Publishes
[(hash(g^XW), g^W, RSSI)]
I-device
I backend server (DP3T)


R backend server (ROBERT)
R-device
R-ECC+EBID
R-ECC+EBID
I-EBIDs
(hash(g^XW), g^W, RSSI)
R-ECC+EBID
I-relay (IDPT)
• Federation with R-backserver
• Publishes
[(hash(g^XW), g^W, RSSI)]
D-device
D backend server (DP3T)
D-EphIDs
D-EphIDs
I-EphIDs
DP3T Flow
R-ECC+EBID
D-EphIDs
I-EBIDs
I-EphIDs
I-device
COVID+
I backend server (DP3T)


R backend server (ROBERT)
R-device
D-device
D backend server (DP3T)
R-ECC+EBID
R-ECC+EBID
I-EBIDs
D-EphIDs
D-EphIDs
I-EphIDs
Infected
EphIDs
(hash(g^XW), g^W, RSSI)
R-ECC+EBID
ROBERT Flow
R-ECC+EBID
D-EphIDs
I-EBIDs
I-EphIDs
I-relay (IDPT)
• Federation with R-backserver
• Publishes
[(hash(g^XW), g^W, RSSI)]
I-device
I backend server (DP3T)
COVID+


R backer server (ROBERT)
Secret W
g^W
R-device
COVID+
D-device
D backend server (DP3T)
R-ECC+EBID
R-ECC+EBID
I-EBIDs
D-EphIDs
D-EphIDs
I-EphIDs
Infected
EphIDs
(hash(g^XW), g^W, RSSI)
I-EBIDs=g^X
R-ECC+EBID
IDPT Flow
R-ECC+EBID
D-EphIDs
I-relay (IDPT)
• Federation with R-backserver
• Publishes
[(hash(g^XW), g^W, RSSI)]
Secret X
I-device
I backend server (DP3T)

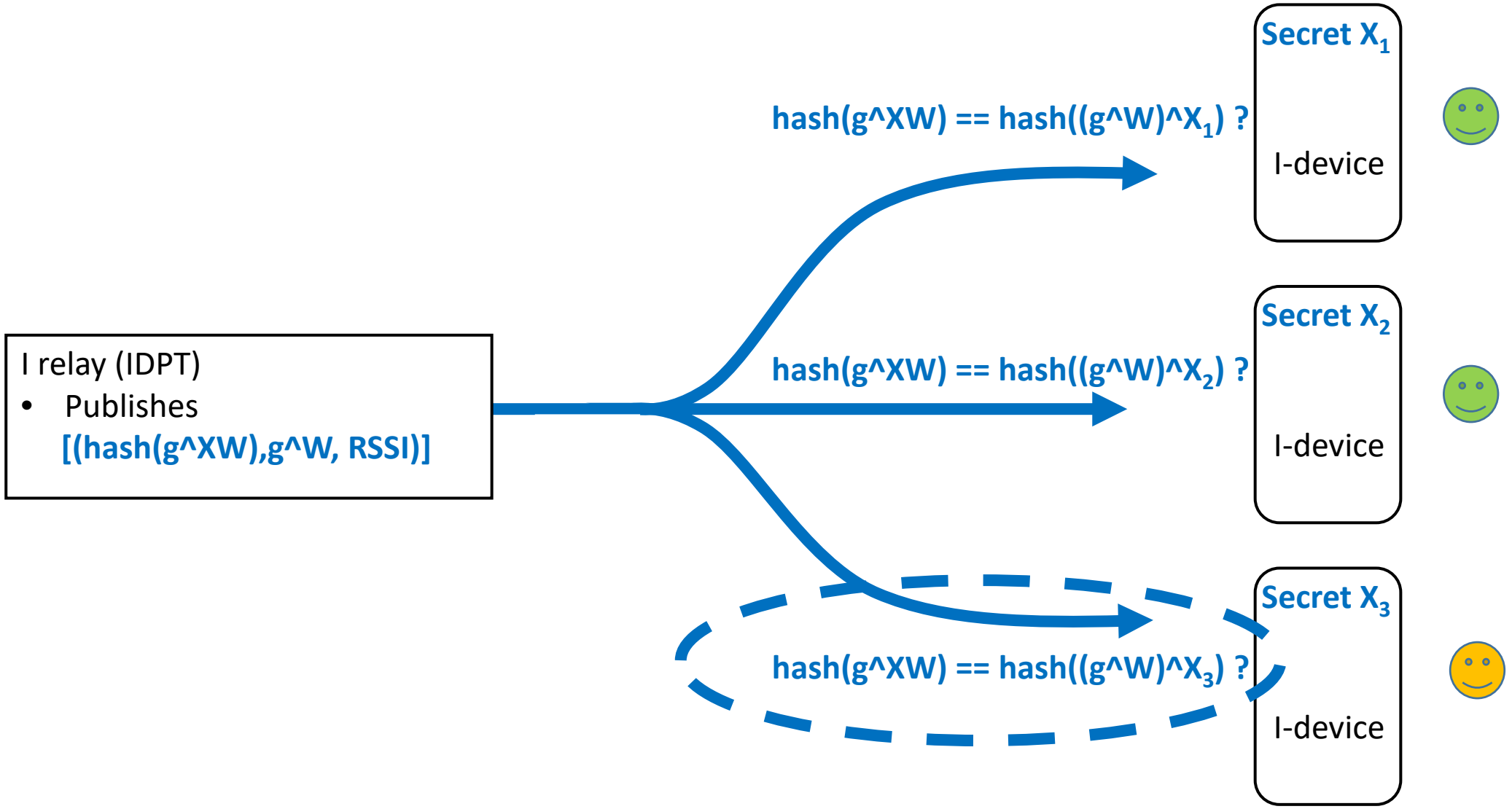
Implementation

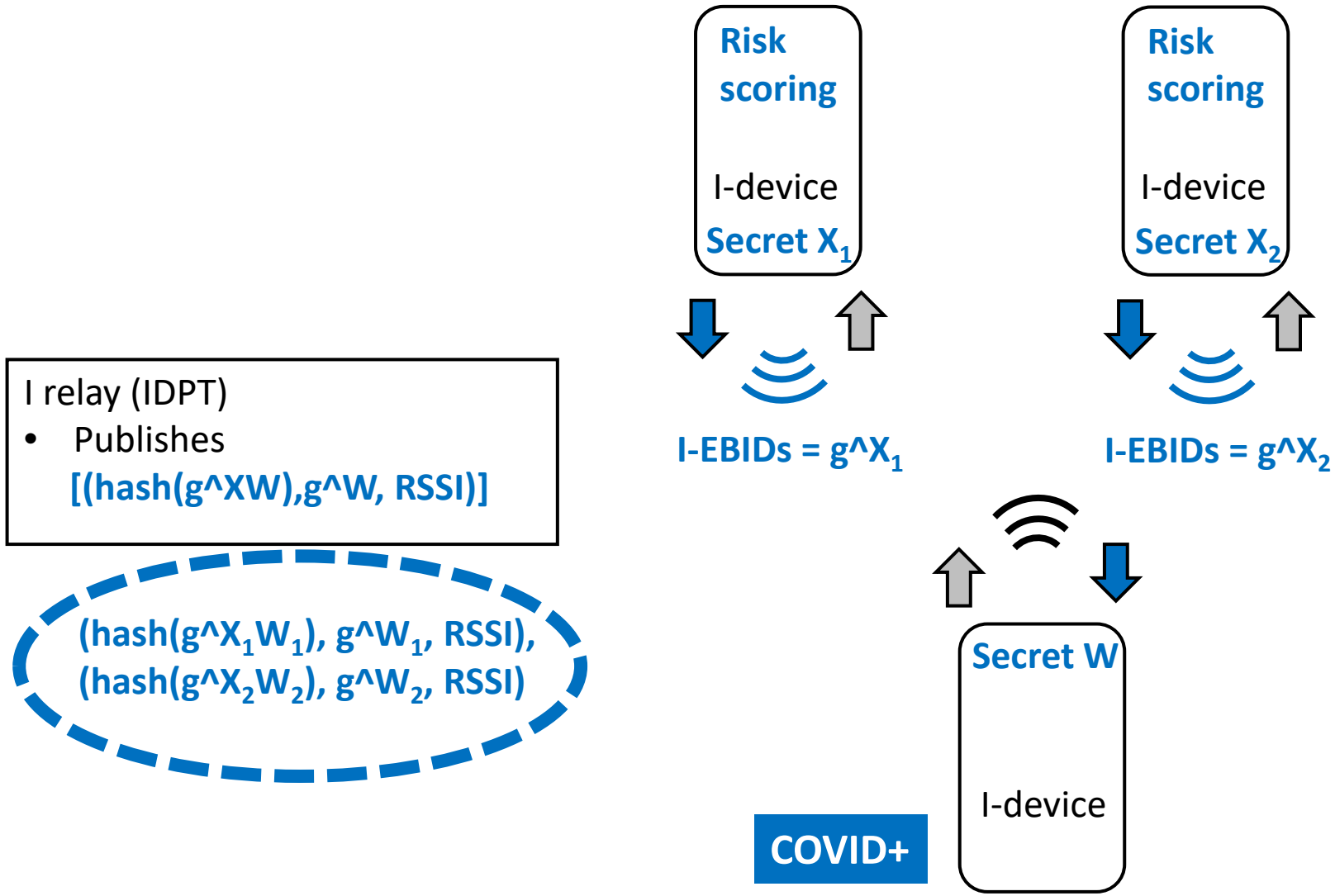
- Modify R apps and R backendserver: *LocalProximityList,* pairs (hash(g^XW), g^W).
- I-devices **generate two types of content for BLE beacons** and must have a faster beacon rate (higher power consumption?, coexistence with EN API BLE beacons?).
- **Generation of g^X beacons not supported by EN API of Gapple**.

Thank you…

Digital proximity tracing protocols

Protocol	Generation of EBID/EphID/PETs	Info provided by COVID+ user	Risk scoring
DP3T	Device	Infected EphIDs	Device
ROBERT	Backserver	Exposed EBIDs	Backserver
DESIRE	Device	Infected/Exposed 2w-PET: Hash(**2-way** contact shared secret)	Backserver
PRONTO	Device	Infected 2w-PET: Hash(**2-way** contact shared secret)	Device
IDPT	Device	Infected 1w-PET: Hash(**1-way** contact shared secret)	Device


I relay (IDPT)
• Publishes
[(hash(g^XW),g^W, RSSI)]
hash(g^XW) == hash((g^W)^X1) ?
hash(g^XW) == hash((g^W)^X2) ?
hash(g^XW) == hash((g^W)^X3) ?
Secret X1
I-device
Secret X2
I-device
Secret X3
I-device


Risk scoring
I-device
Secret X_1
Risk scoring
I-device
Secret X_2
I-EBIDs = g^X_1
I-EBIDs = g^X_2
I relay (IDPT)
• Publishes
[(hash(g^XW),g^W, RSSI)]
(hash(g^X_1W_1), g^W_1, RSSI),
(hash(g^X_2W_2), g^W_2, RSSI)
Secret W
I-device
COVID+