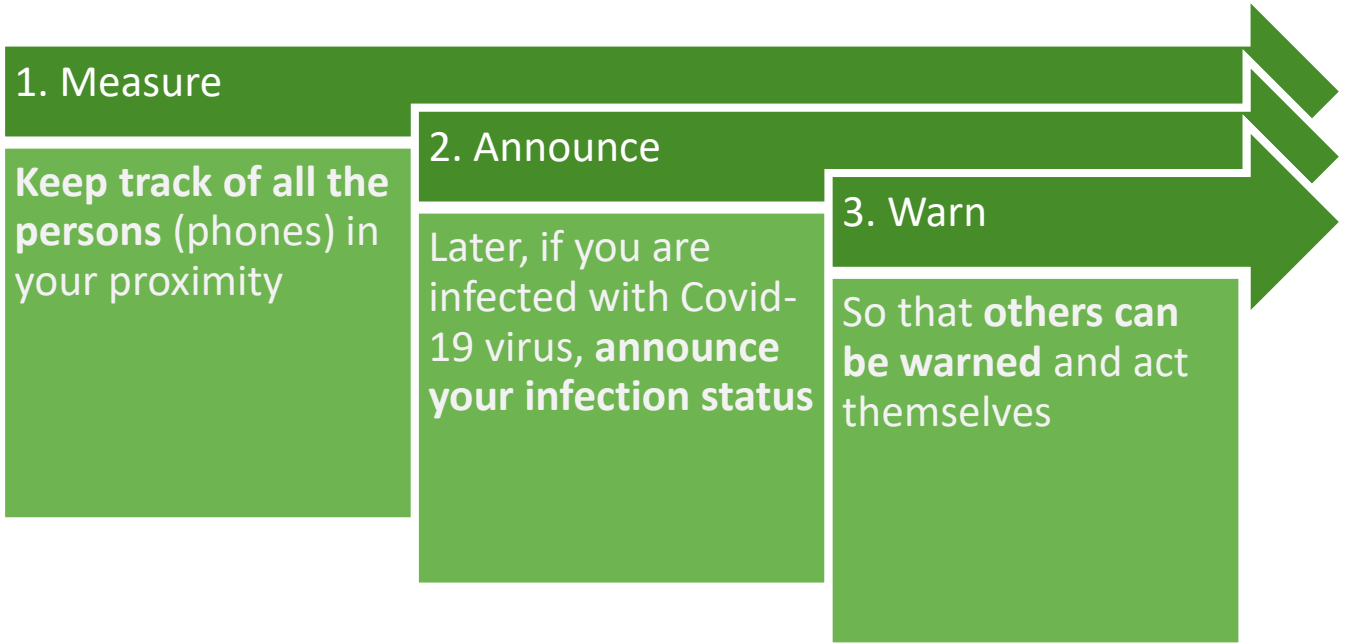
AUTORITEIT
PERSOONSGEGEVENS

Google/Apple Exposure Notification framework

October 2020

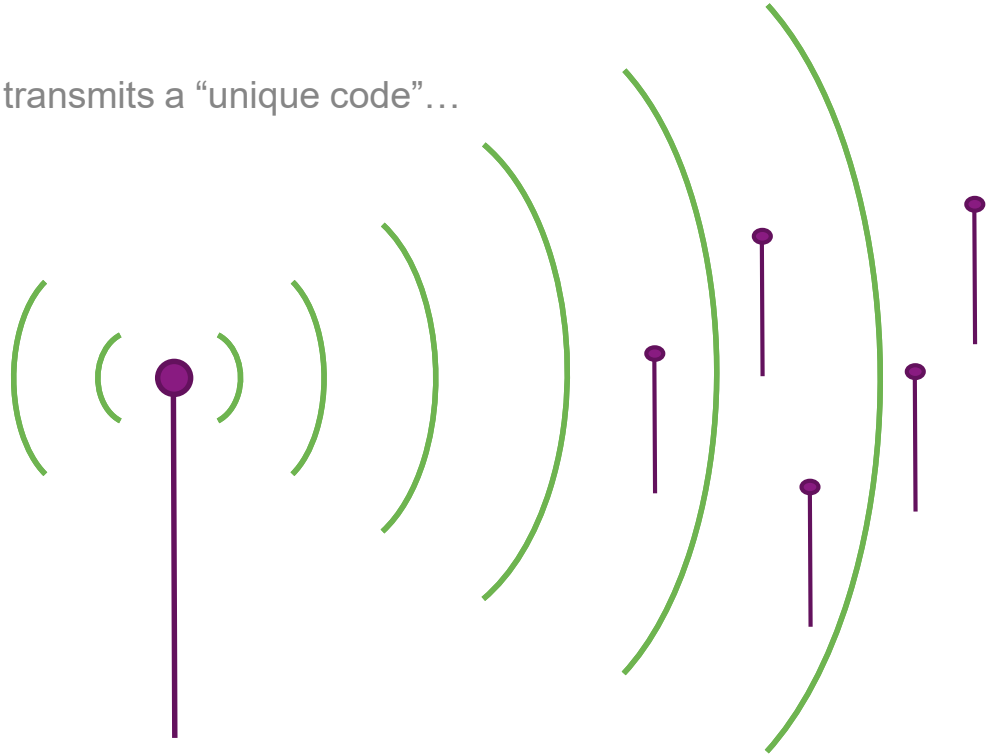
Exposure Notification is a multi-step process



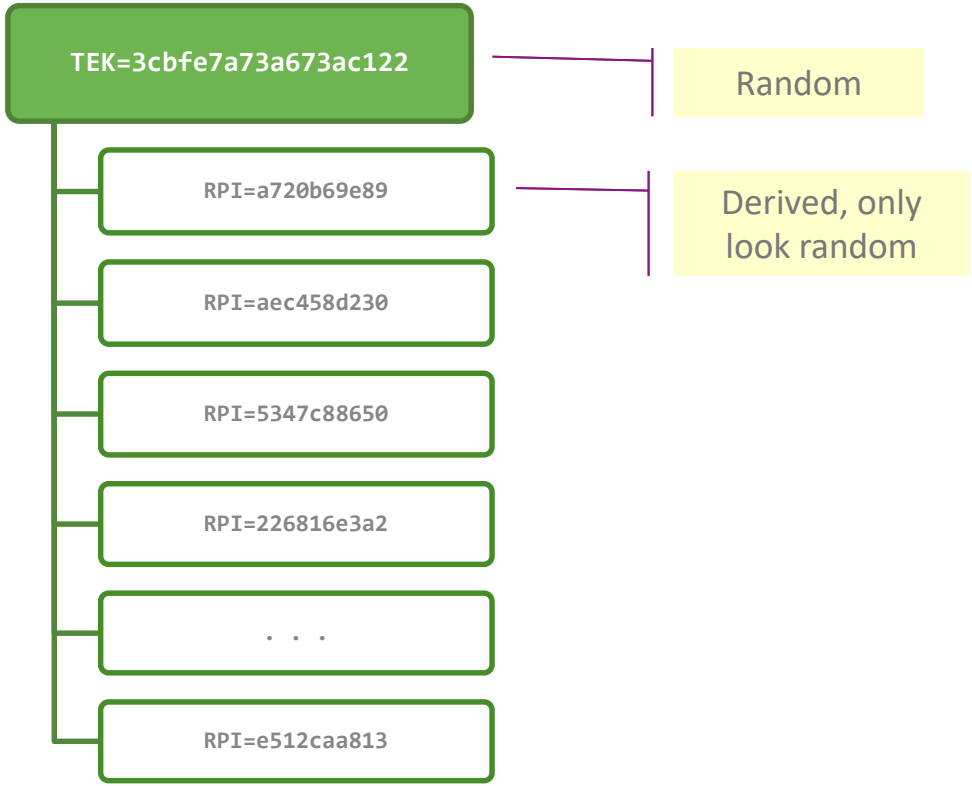
Schematically

Every phone transmits a “unique code”…

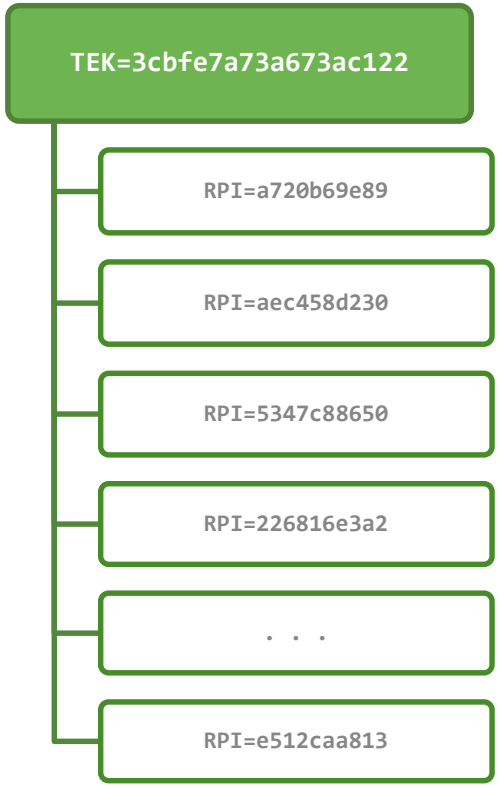
… that is received by all phones nearby



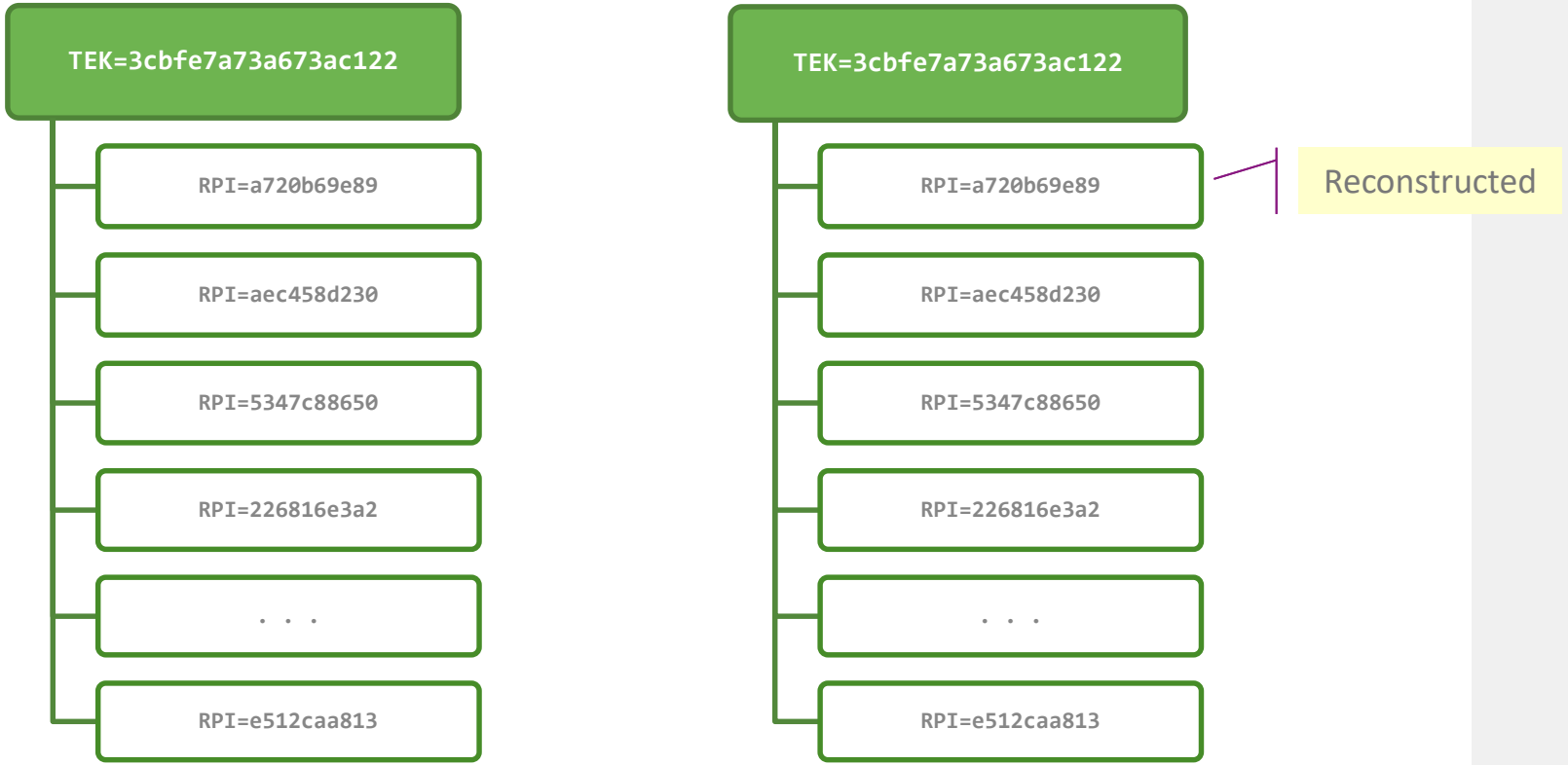
“Random Codes”



“Random Codes”



“Random Codes”



Personal data involved

Data	Pseudonymous Identifier?	Health Data?
Temporary Exposure Keys	✓	
Rolling Proximity Identifiers	✓	
Diagnosis Keys	✓	✓
Exposure Risk		✓

As outlined by the EDPB in the interoperability statement

Privacy by Design

- The proximity identifiers rotate every 10-20 minutes
- Calculating the *Exposure Risk Score* is done on the phone, not in the cloud
- The app cannot be used as a “Covid Passport”
  to prove ones infection status (NL-specific)

Not so Private by Design

- TEK's don't change often enough
- Exposure Notification is a framework that tracks who meets who in real life, on an unprecedented scale, embedded in closed-source operating systems/middleware
  [Do you spend time with your spouse? Are you risk aversive?]
- The calculation of the Exposure Risk Score happens inside the framework, not in the app. Thus the framework learns all health data involved (telemetry?!)
  [The threat model of Google/Apple is "don't trust the app"]

Forward

As soon as possible: go into detail
- Better explain: DPbD ≠ anonimity
- Telemetry? Legal safeguards necessary? On European level?
- Can GA change the API boundary between framework and app? Will they?
- Is Exposure Notification “just another API”? How about phase II?

For the bold:
- Address governance

Next time:
- invite Health Authorities and Data Protection Authorities to design phase