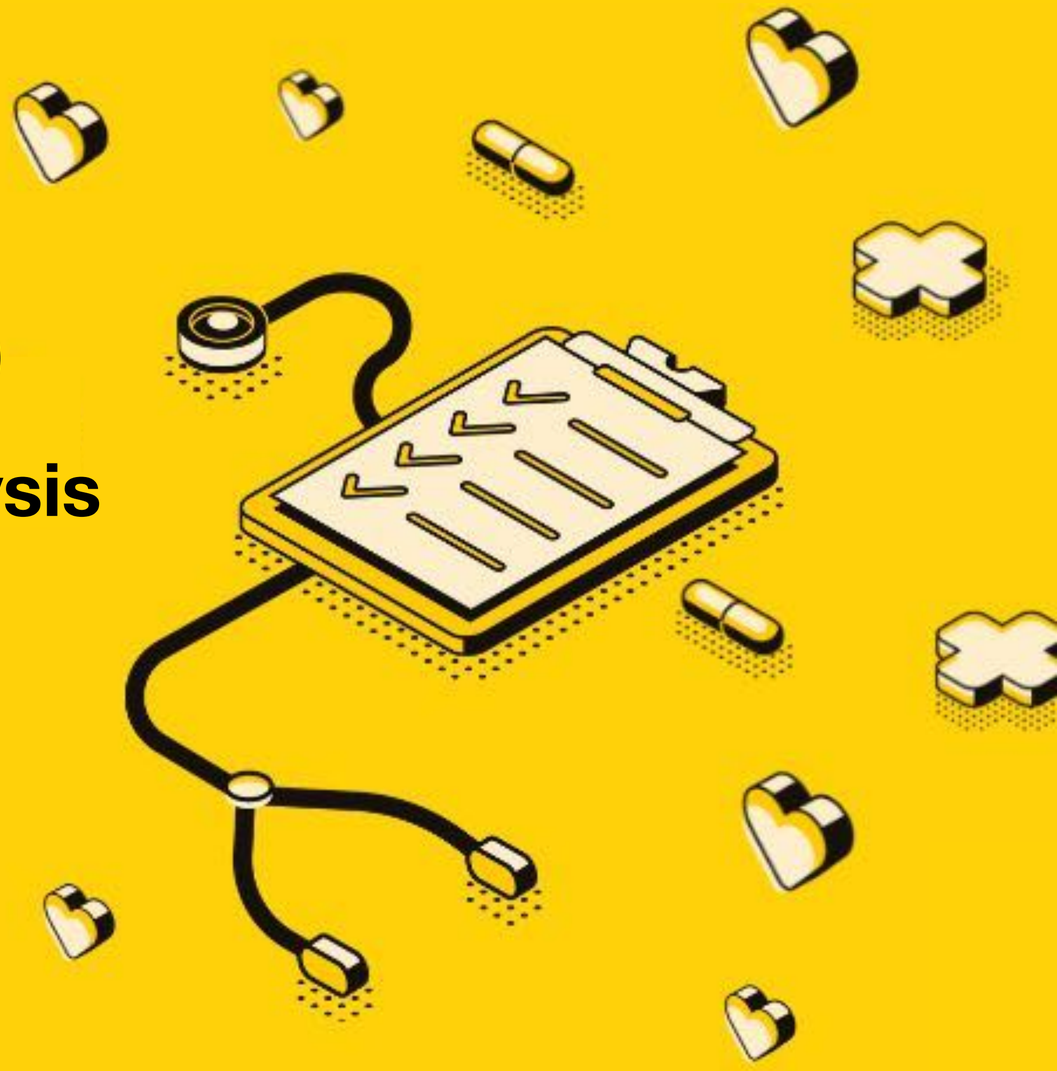
iOS FHE Demo App

Build a Privacy-Preserving Health Analysis iOS Mobile App Using TFHE-rs



Dimitri Dupuis-Latour - Sept 28, 2024

Presentation

Dimitri Dupuis-Latour

- Freelance iOS Developer
- @Zama for a short mission, exploring FHE on iPhone
- Formerly at Apple (Xcode Developer Tools)
- Developed numerous mobile, B2C apps over the years: BeReal, TF1, PMU, Kering, L’Oréal, YSL, My Little Paris…

Mobile Apps Landscape

Privacy is paramount

- Smartphones are ubiquitous
- Mobile apps can access lot of personal data:
  - hardware sensors (camera, microphone, GPS…)
  - user data (contacts, health info…)
- Privacy is a concern
- We can do better at preserving user privacy

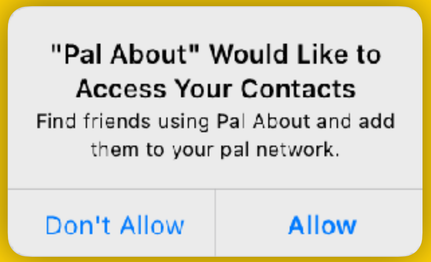
Permission Dialogs

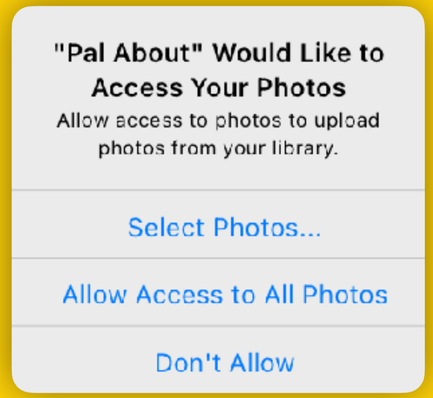
Current solution

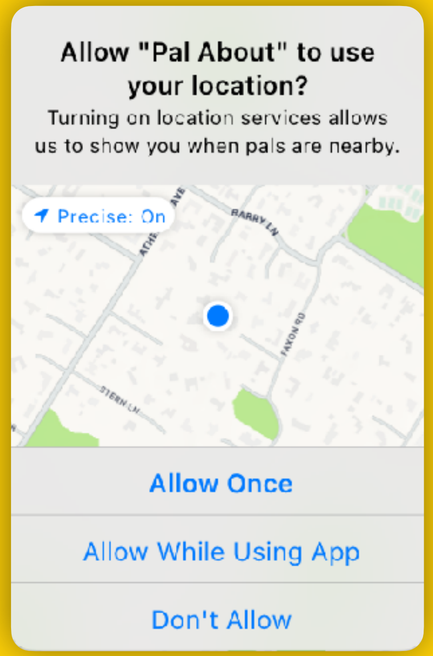
Permission Dialogs

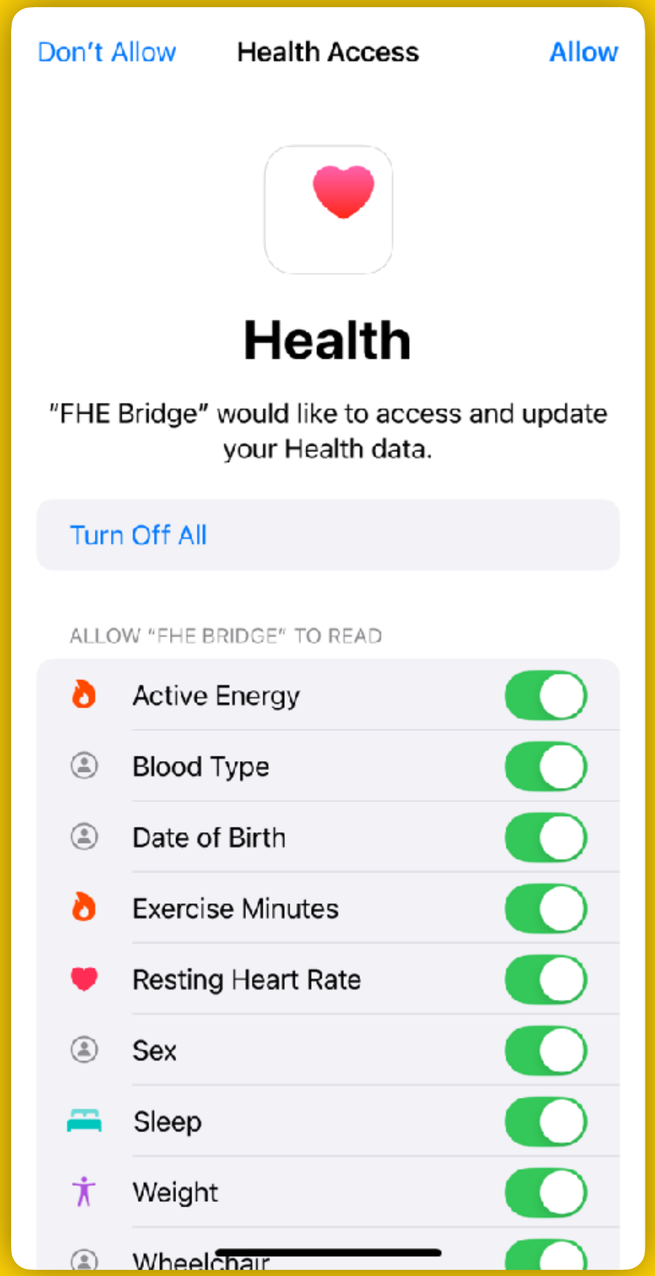
Current solution

- Access to sensors and data is gated through Apple’s APIs
- Permission dialogs are triggered to grant access, with granular control
- Users can revoke access anytime through the Settings app


"Pal About" Would Like to Access Your Contacts
Find friends using Pal About and add them to your pal network.
Don't Allow
Allow


"Pal About" Would Like to Access Your Photos
Allow access to photos to upload photos from your library.
Select Photos...
Allow Access to All Photos
Don't Allow


Allow "Pal About" to use your location?
Turning on location services allows us to show you when pals are nearby.
Precise: On
Allow Once
Allow While Using App
Don't Allow


Don't Allow
Health Access
Allow
Health
"FHE Bridge" would like to access and update your Health data.
Turn Off All
ALLOW "FHE BRIDGE" TO READ
Active Energy
Blood Type
Date of Birth
Exercise Minutes
Resting Heart Rate
Sex
Sleep
Weight
Wheelchair

Permission Dialogs

Limitations

- **Clear text access**: Once permission is granted, apps access data in plain text
- **Dialog fatigue**: Users often click "Yes" without checking
- **Dialog friction**: Can cause app anxiety, and lead users to deny legitimate requests

Privacy-gating, not privacy-preserving

FHE Encrypted APIs

Proposed architecture

Introducing FHE-based APIs

- In a world with FHE-based iOS APIs:
  - Sensitive data is returned in FHE-encrypted form, not clear text
  - Apps can process data without being able to read it
  - No permission dialogs: Apps could access encrypted data without privacy risk

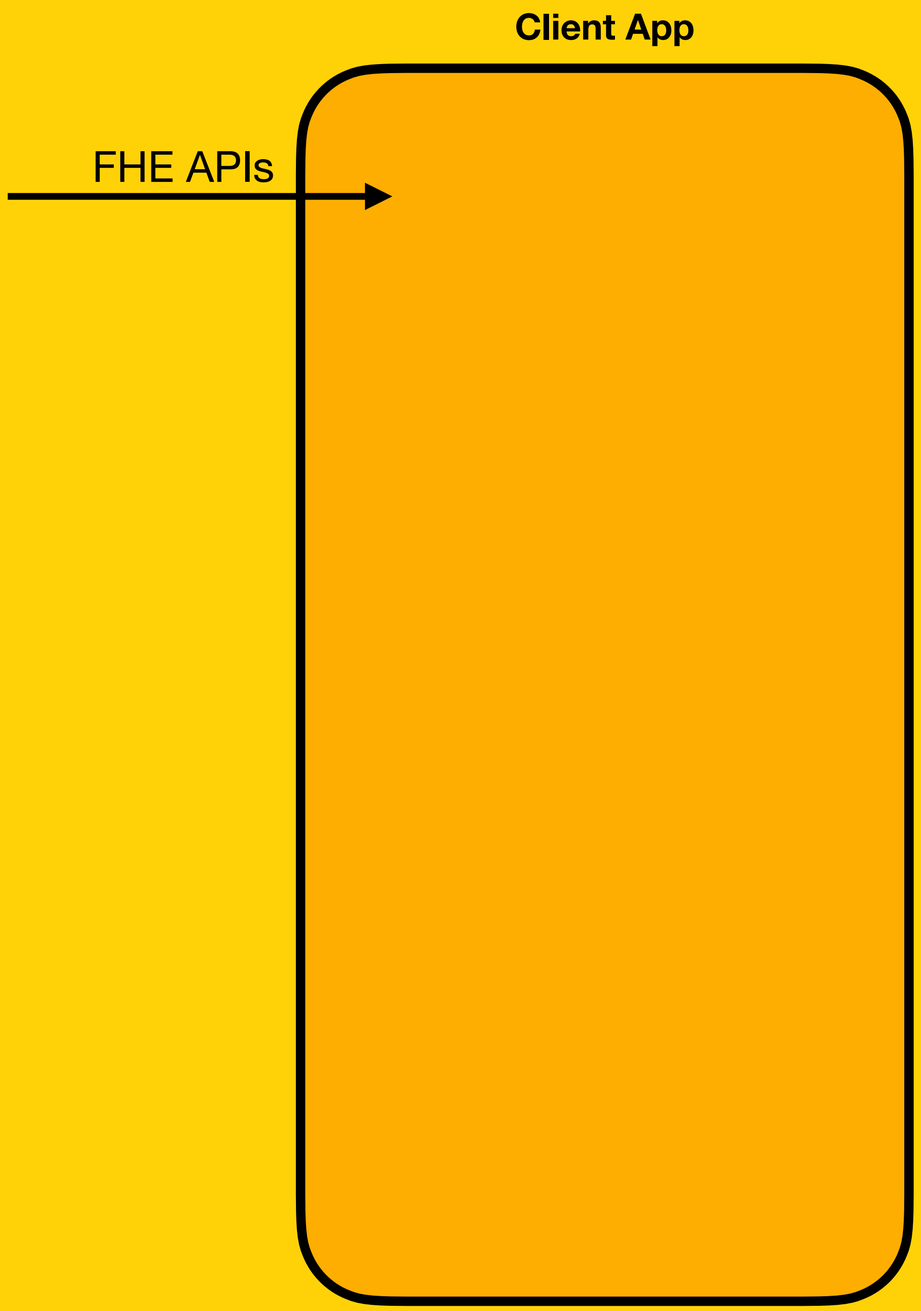
The Tricky Part: Rendering Result

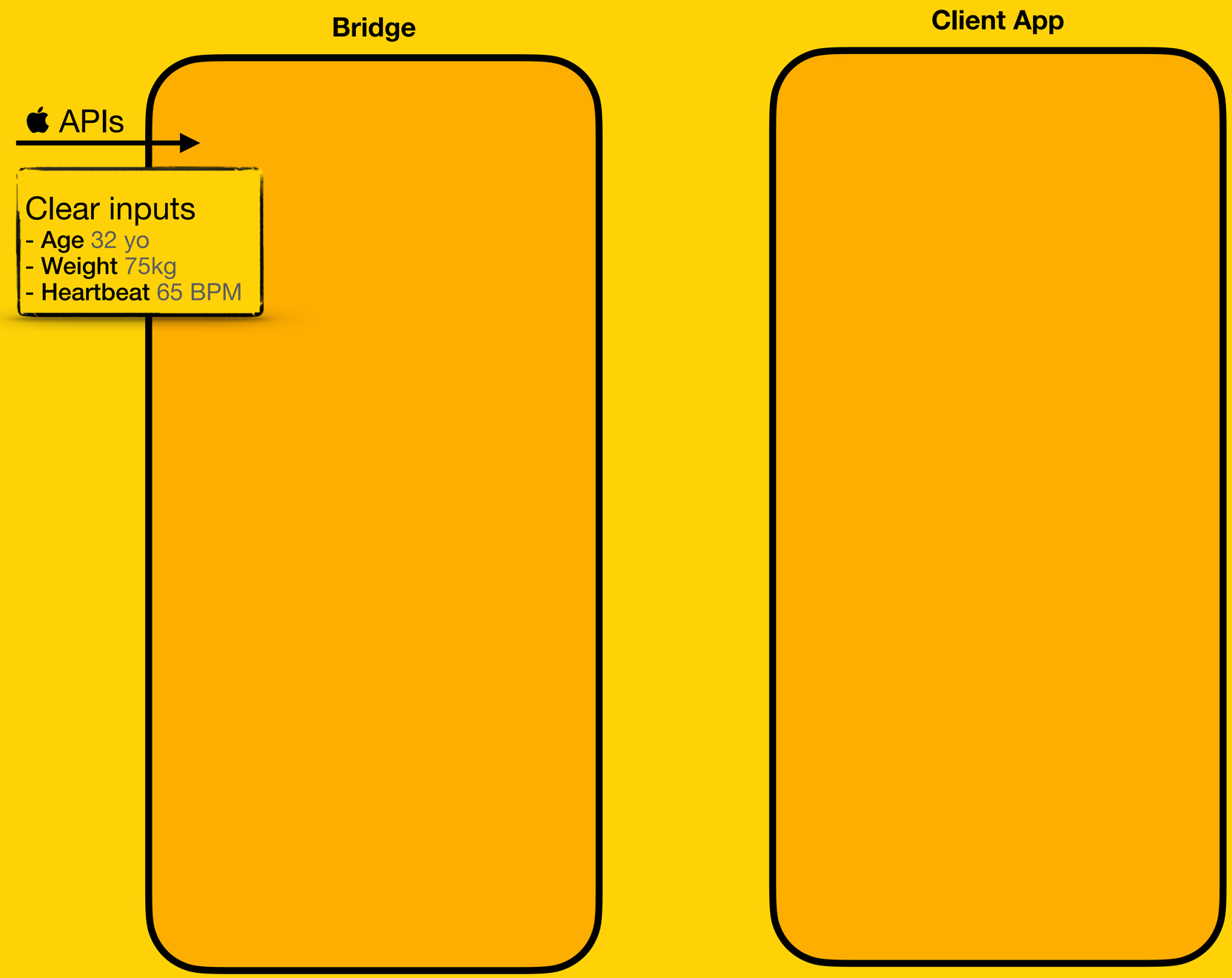
- FHE computation can be done on the phone or on a server
- The user wants to see decrypted results, but who decrypts them?
  - Either the app: but risk of accessing clear text data
  - Or in the OS: better security but less flexibility for apps, and Zama doesn't control the OS

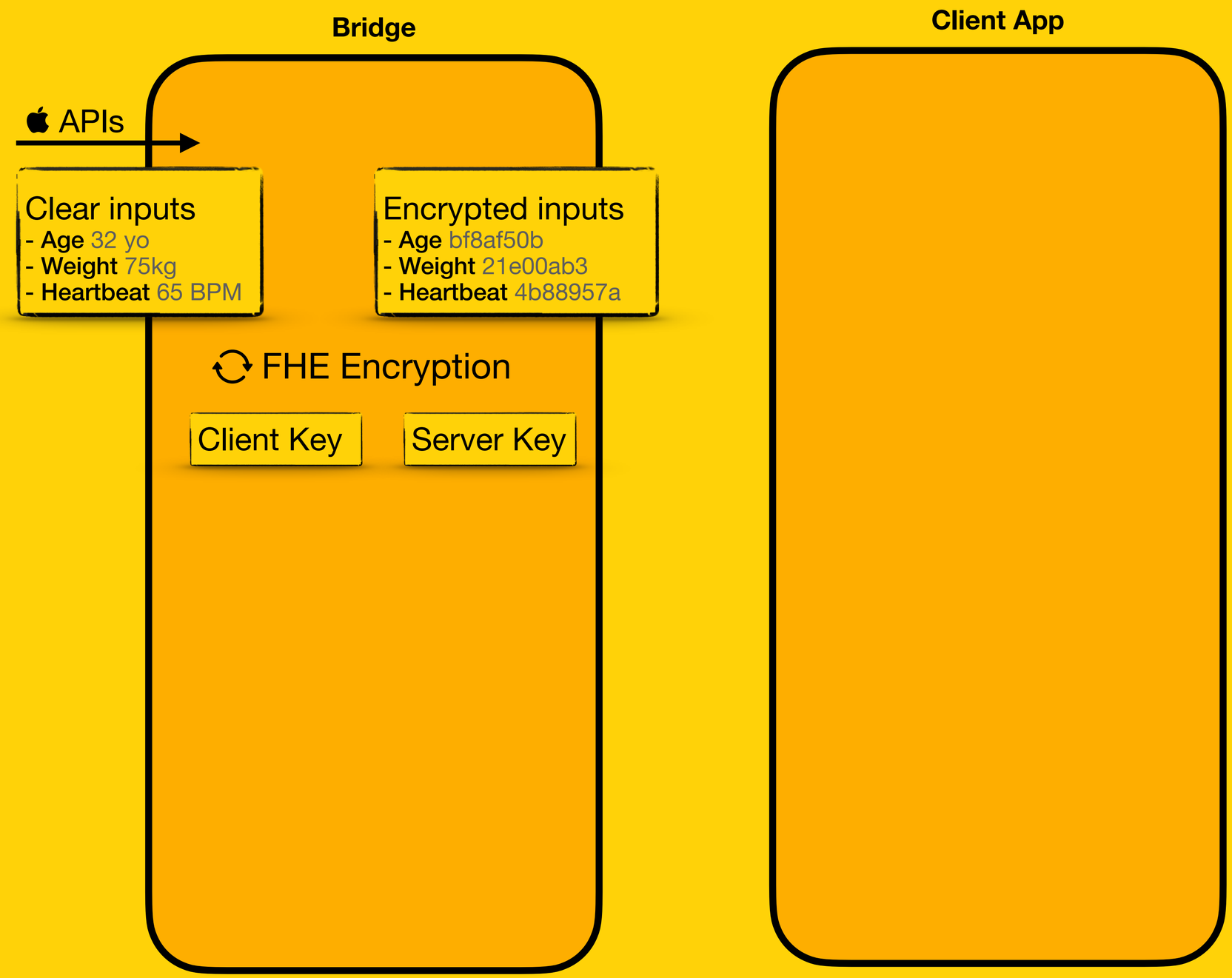
Solution: Private View

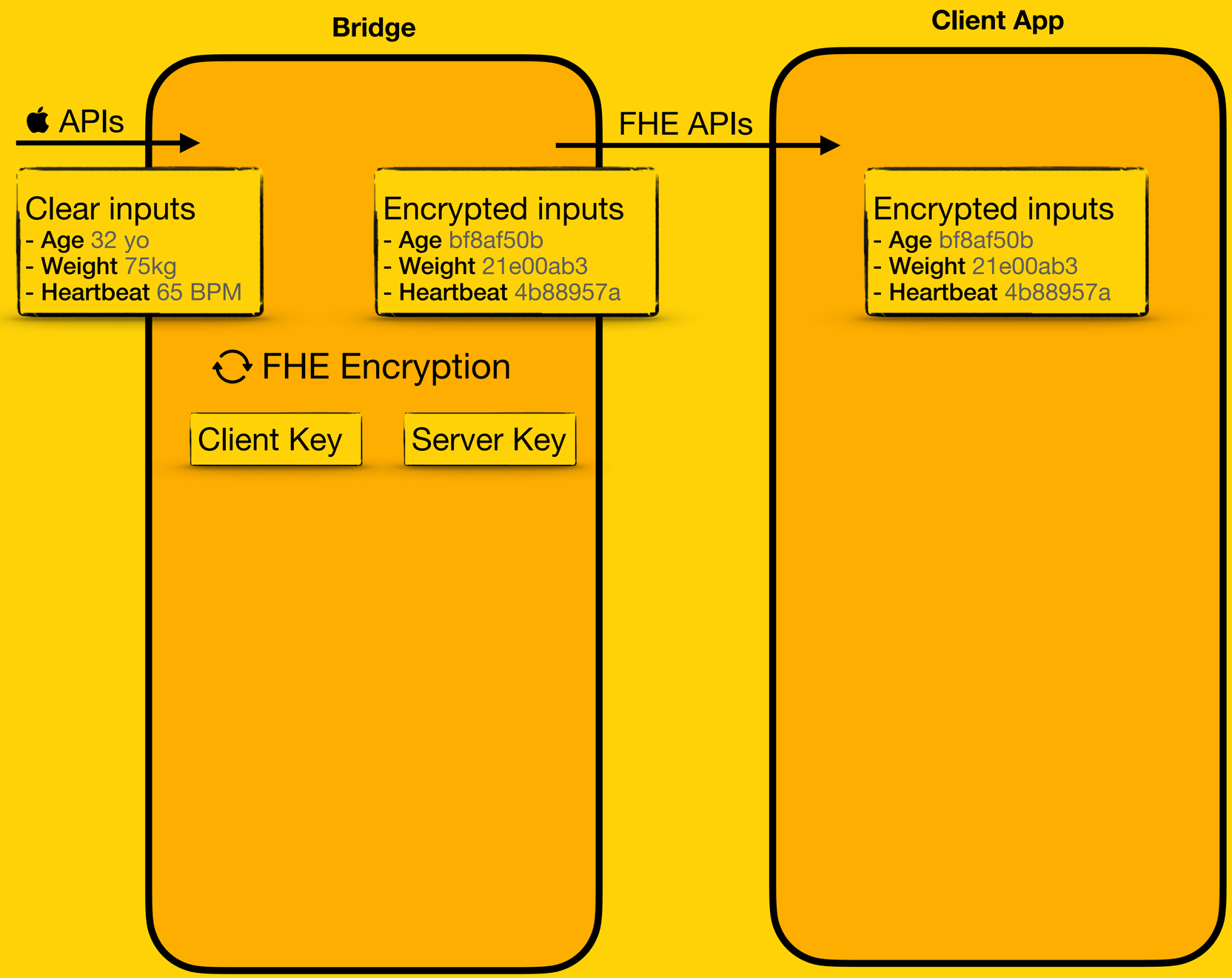
- A private view works like an iframe or black box
- **Visible to the user** but hidden from the app
- The app can display the result without accessing the decrypted data

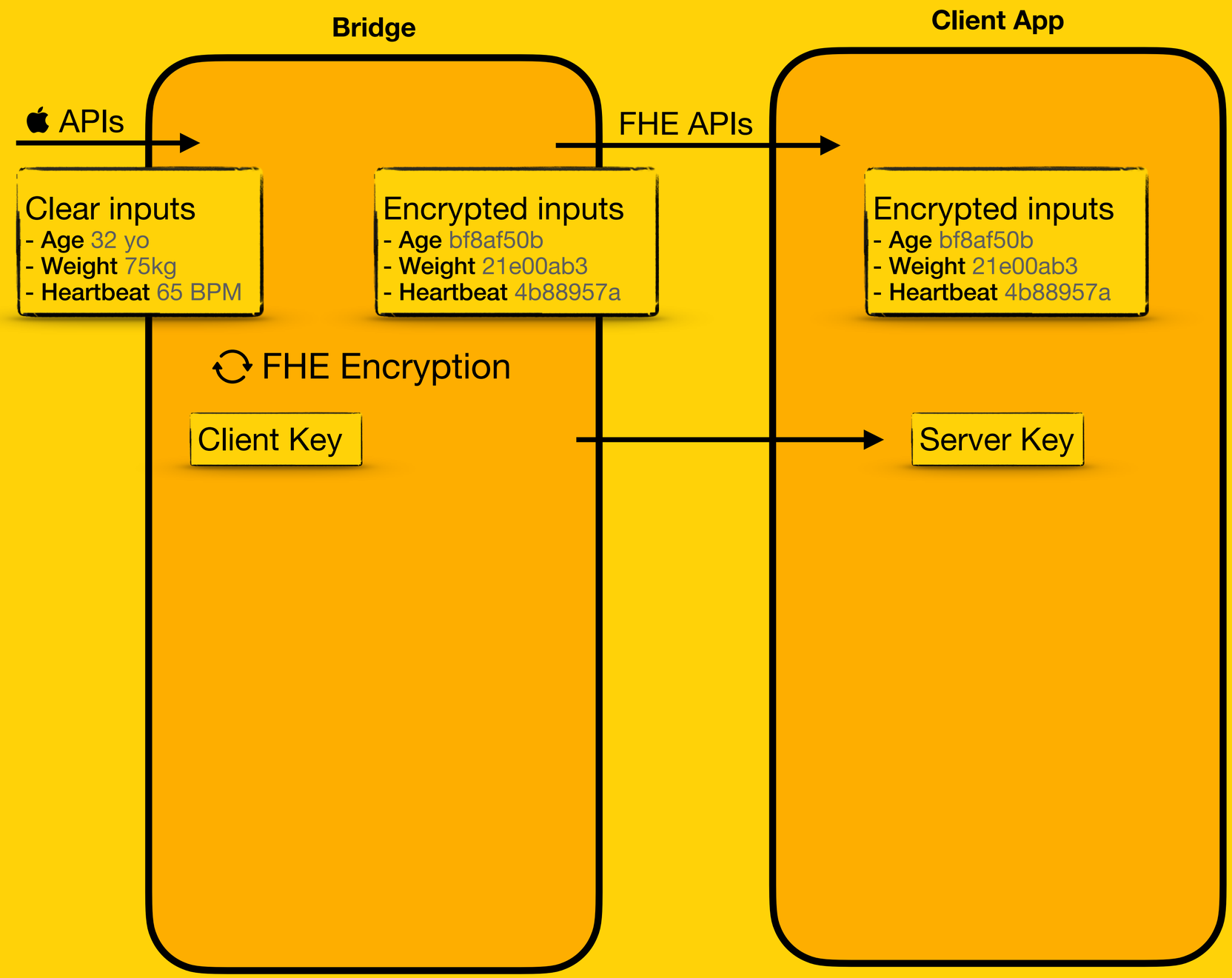
Workflow

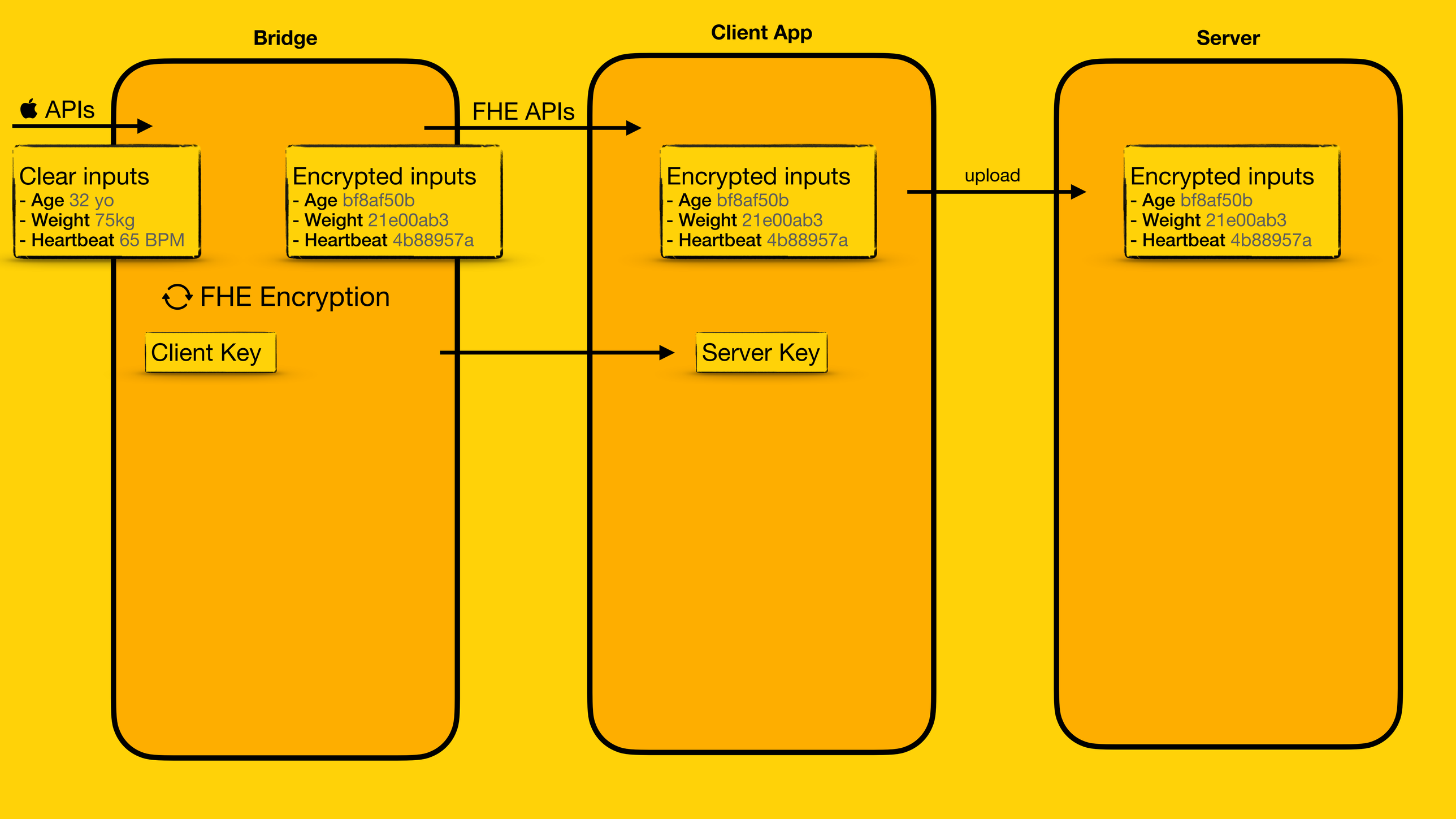

Client App
FHE APIs

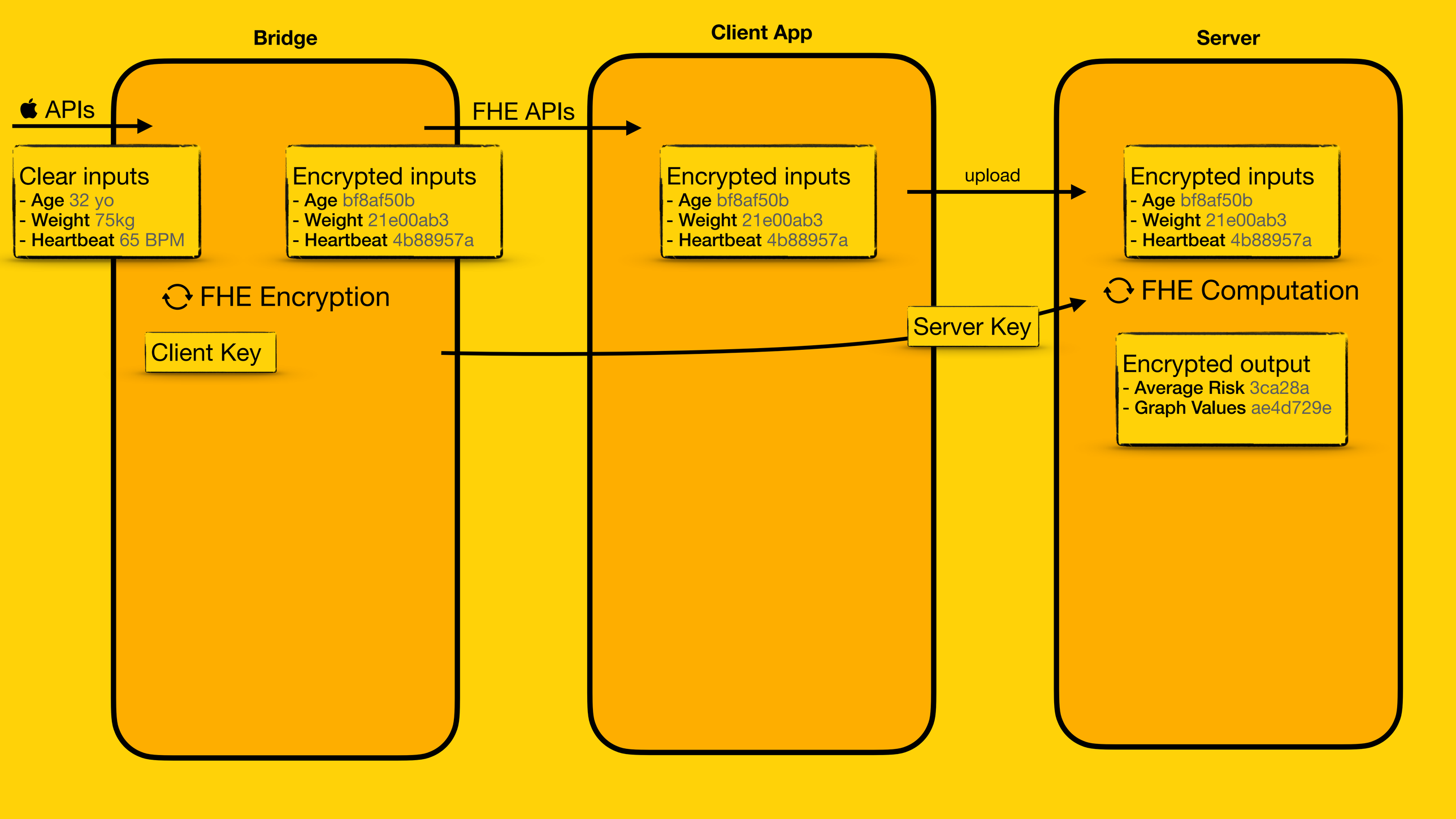

Bridge
Client App
APIs
Clear inputs
- Age 32 yo
- Weight 75kg
- Heartbeat 65 BPM

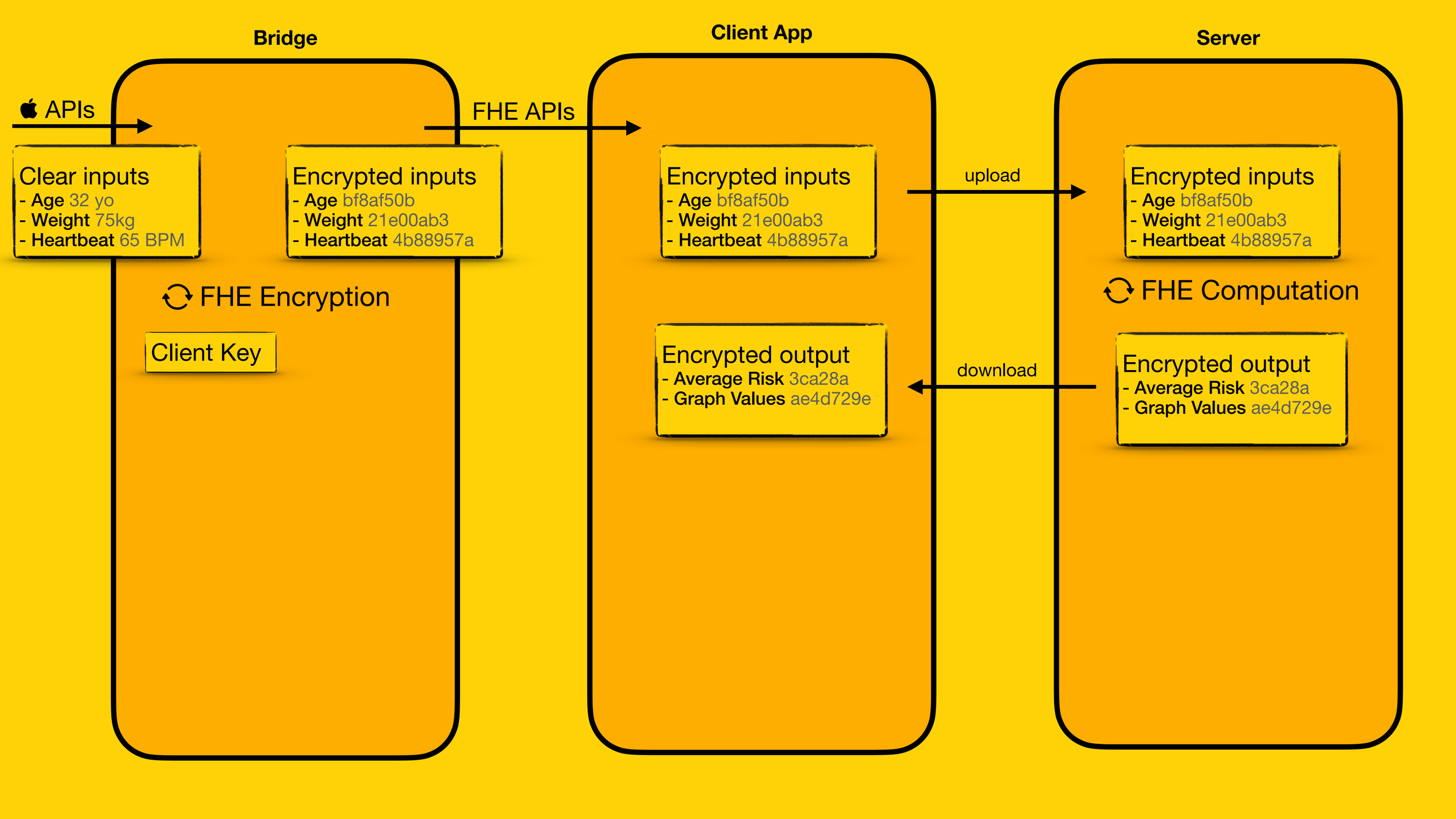

Bridge
Client App
APIs
Clear inputs
- Age 32 yo
- Weight 75kg
- Heartbeat 65 BPM
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Encryption
Client Key
Server Key

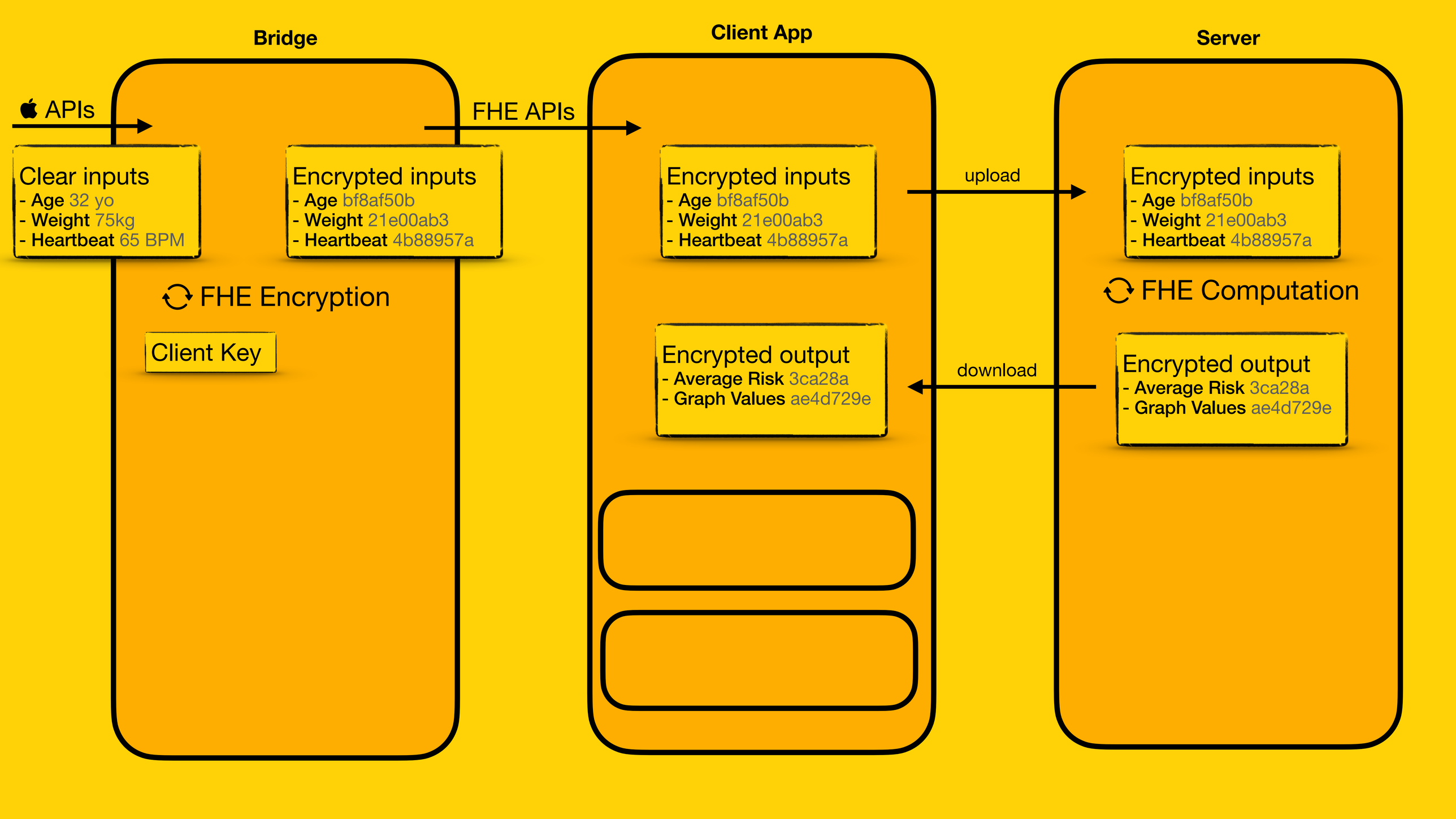

Bridge
Client App
APIs
FHE APIs
Clear inputs
- Age 32 yo
- Weight 75kg
- Heartbeat 65 BPM
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Encryption
Client Key
Server Key

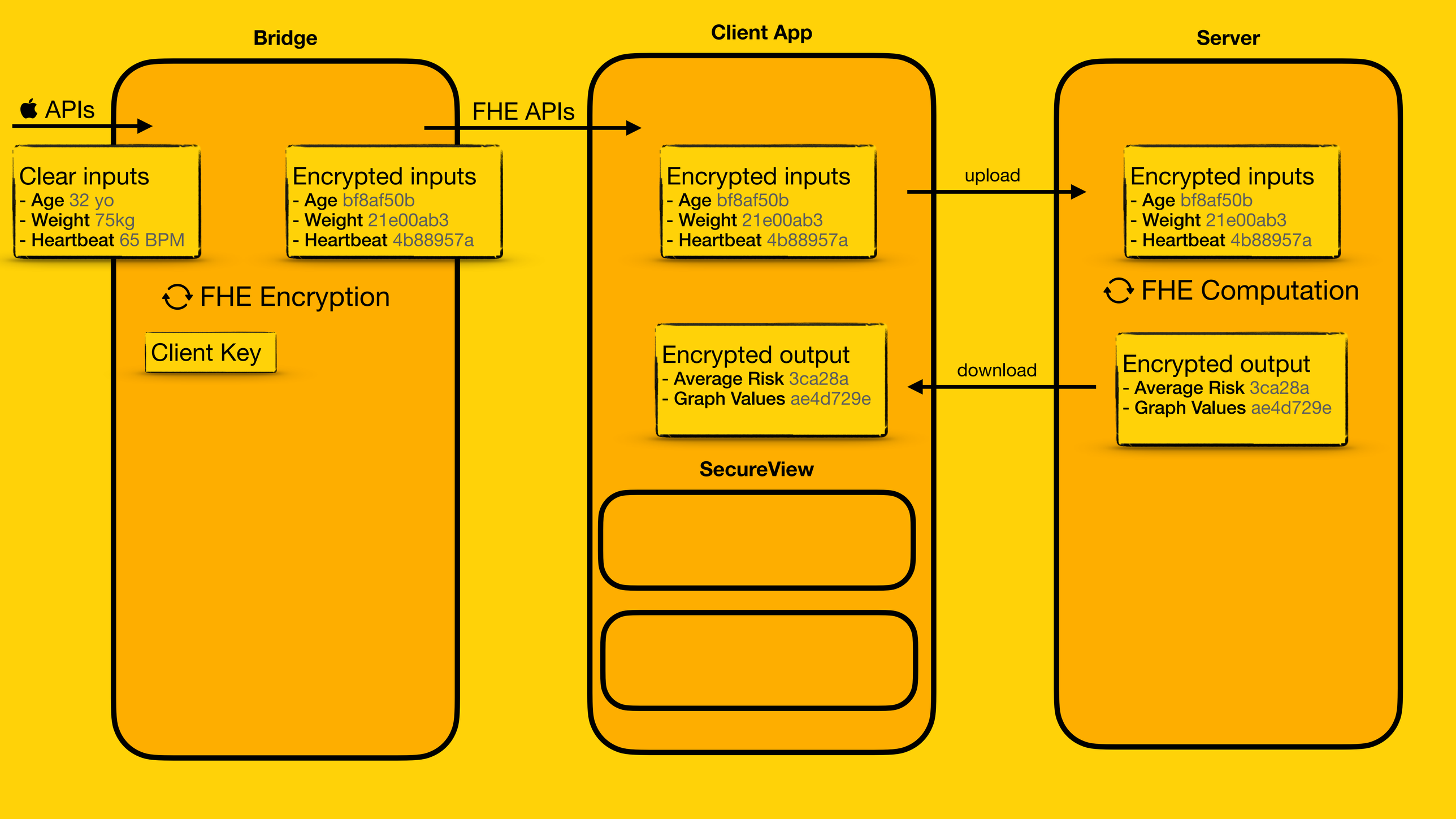

Bridge
Client App
APIs
FHE APIs
Clear inputs
- Age 32 yo
- Weight 75kg
- Heartbeat 65 BPM
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Encryption
Client Key
Server Key

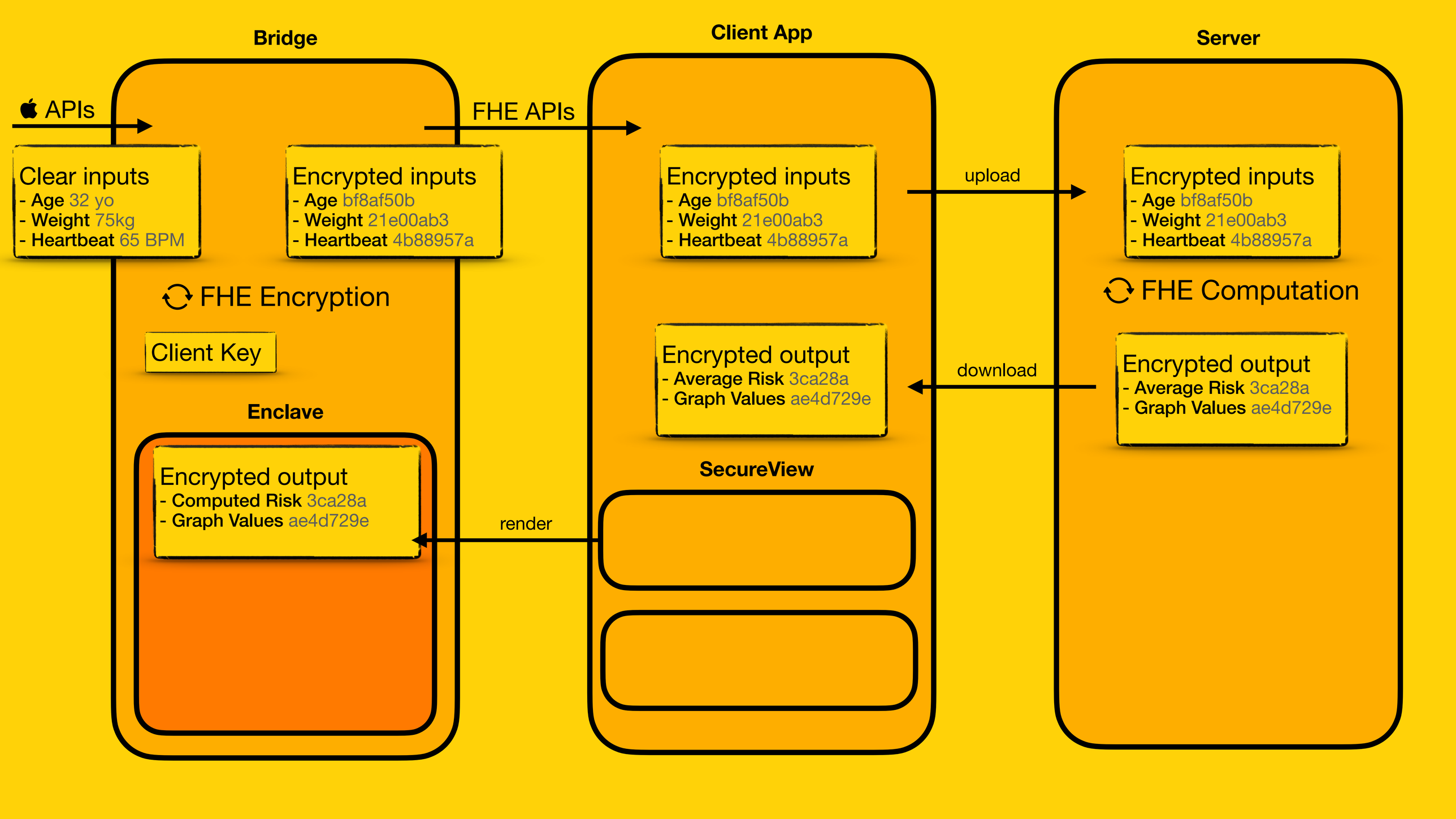

Bridge
Client App
Server
APIs
FHE APIs
Clear inputs
- Age 32 yo
- Weight 75kg
- Heartbeat 65 BPM
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
upload
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Encryption
Client Key
Server Key

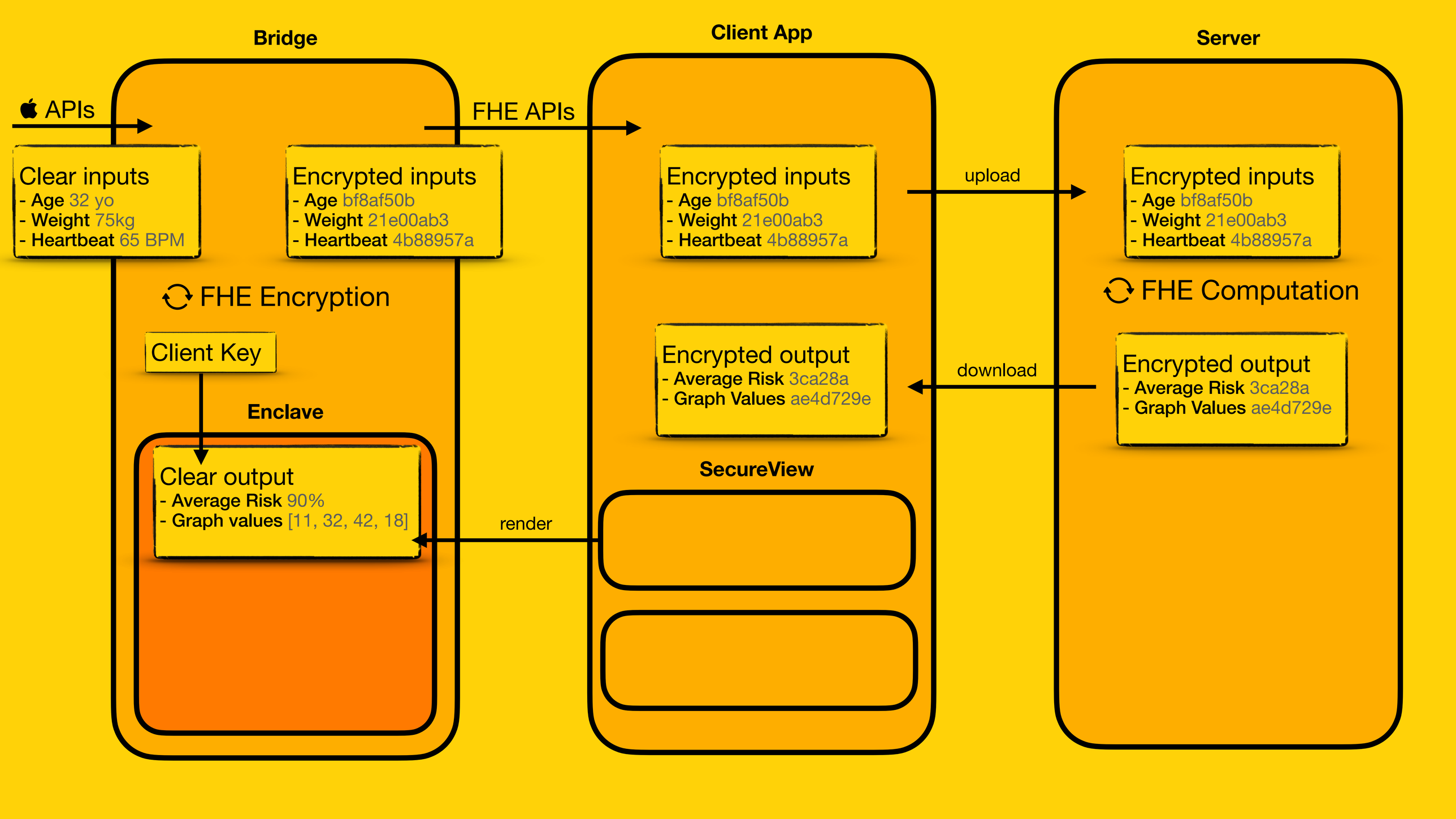

Bridge
Client App
Server
APIs
FHE APIs
Clear inputs
- Age 32 yo
- Weight 75kg
- Heartbeat 65 BPM
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Encryption
Client Key
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
upload
Server Key
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Computation
Encrypted output
- Average Risk 3ca28a
- Graph Values ae4d729e

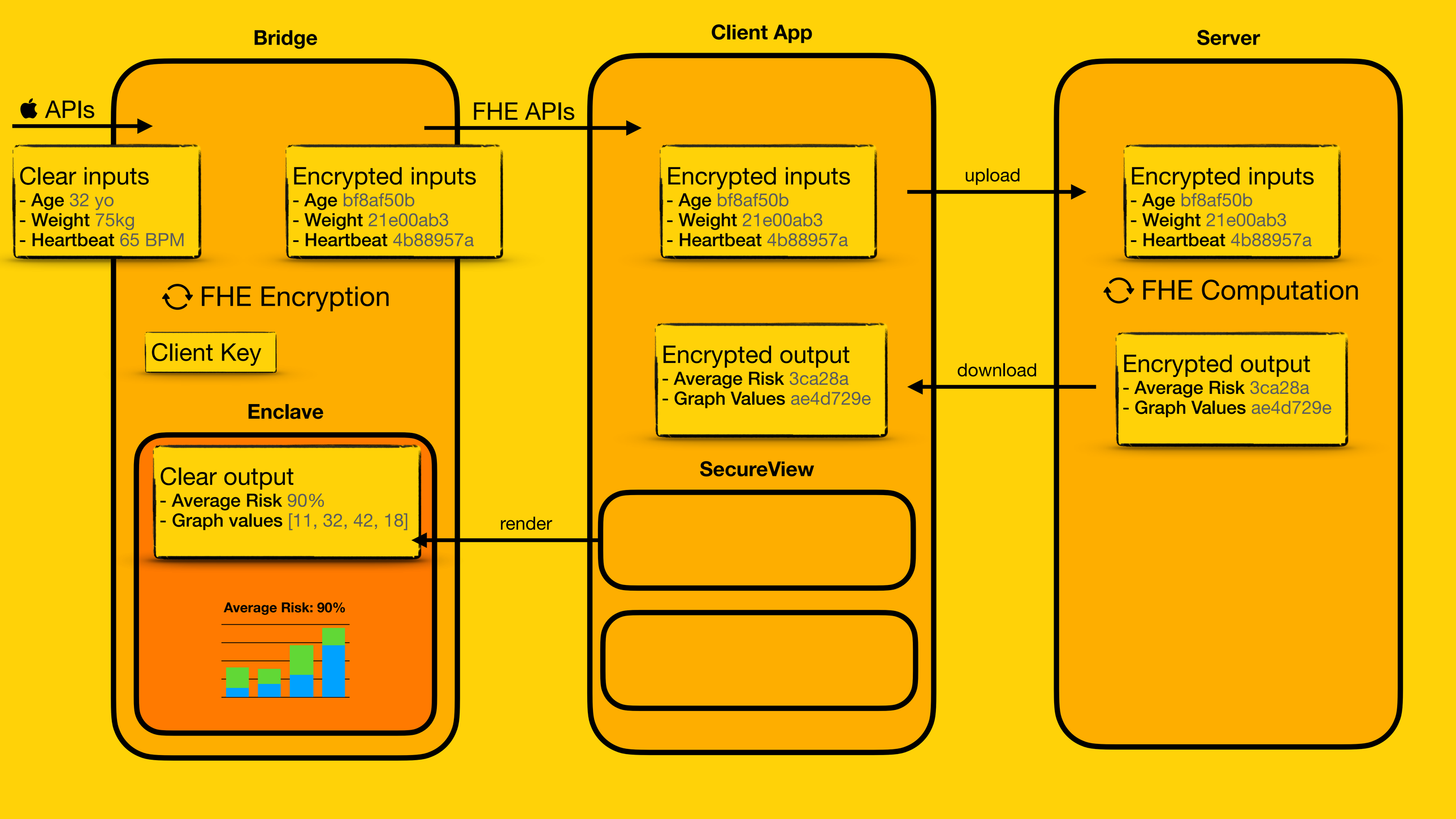

Bridge
Client App
Server
APIs
FHE APIs
Clear inputs
- Age 32 yo
- Weight 75kg
- Heartbeat 65 BPM
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Encryption
Client Key
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
Encrypted output
- Average Risk 3ca28a
- Graph Values ae4d729e
upload
download
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Computation
Encrypted output
- Average Risk 3ca28a
- Graph Values ae4d729e

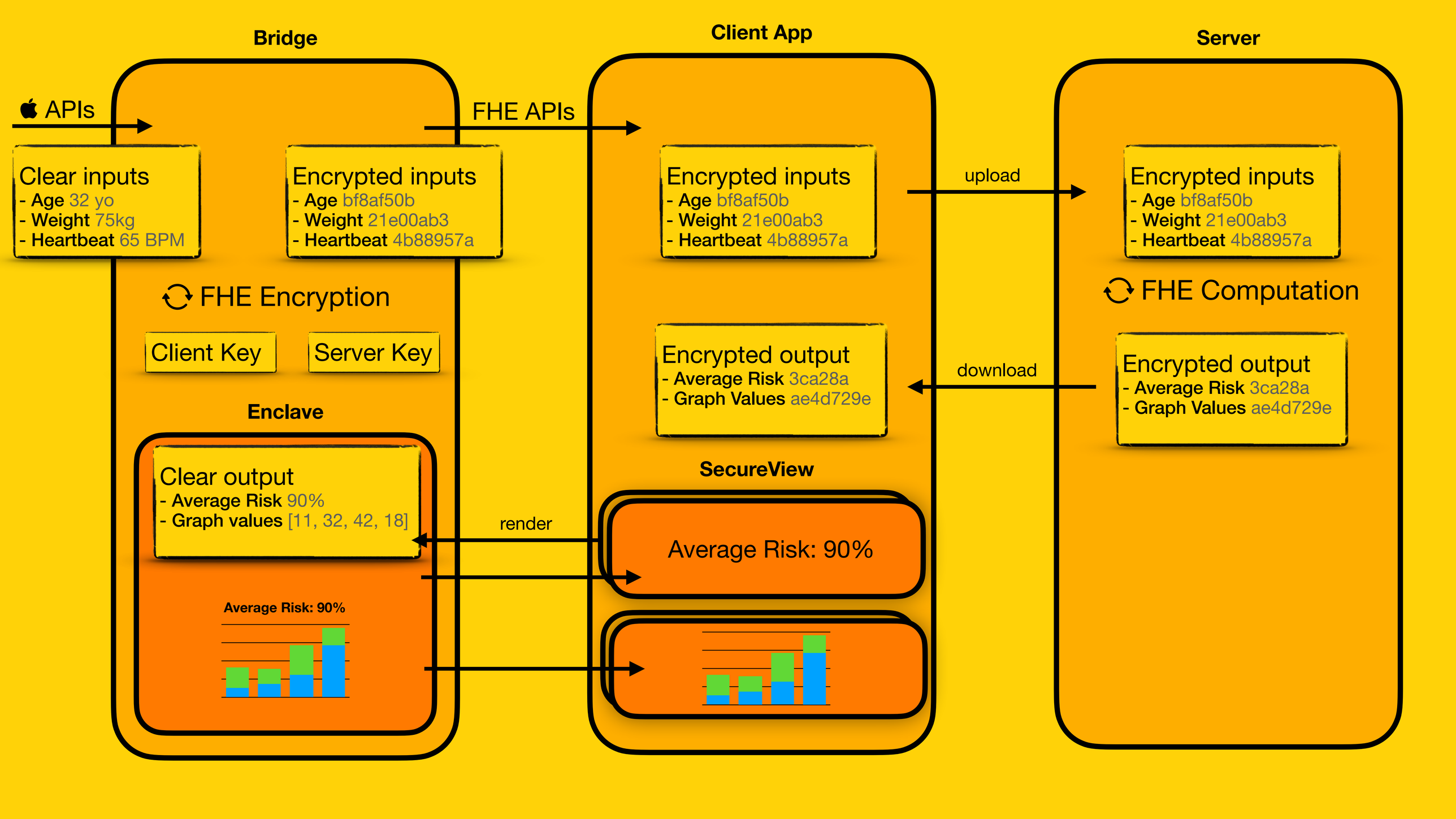

Bridge
Client App
Server
APIs
FHE APIs
Clear inputs
- Age 32 yo
- Weight 75kg
- Heartbeat 65 BPM
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Encryption
Client Key
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
upload
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Computation
Encrypted output
- Average Risk 3ca28a
- Graph Values ae4d729e
download
Encrypted output
- Average Risk 3ca28a
- Graph Values ae4d729e


Bridge
Client App
Server
APIs
FHE APIs
Clear inputs
- Age 32 yo
- Weight 75kg
- Heartbeat 65 BPM
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Encryption
Client Key
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
upload
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Computation
Encrypted output
- Average Risk 3ca28a
- Graph Values ae4d729e
download
Encrypted output
- Average Risk 3ca28a
- Graph Values ae4d729e
SecureView


Bridge
Client App
Server
APIs
FHE APIs
Clear inputs
- Age 32 yo
- Weight 75kg
- Heartbeat 65 BPM
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Encryption
Client Key
Enclave
Encrypted output
- Computed Risk 3ca28a
- Graph Values ae4d729e
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
Encrypted output
- Average Risk 3ca28a
- Graph Values ae4d729e
SecureView
upload
download
render
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Computation
Encrypted output
- Average Risk 3ca28a
- Graph Values ae4d729e


Bridge
Client App
Server
APIs
FHE APIs
Clear inputs
- Age 32 yo
- Weight 75kg
- Heartbeat 65 BPM
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Encryption
Client Key
Enclave
Clear output
- Average Risk 90%
- Graph values [11, 32, 42, 18]
render
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
Encrypted output
- Average Risk 3ca28a
- Graph Values ae4d729e
SecureView
upload
download
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Computation
Encrypted output
- Average Risk 3ca28a
- Graph Values ae4d729e


Bridge
Client App
Server
APIs
FHE APIs
Clear inputs
- Age 32 yo
- Weight 75kg
- Heartbeat 65 BPM
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Encryption
Client Key
Enclave
Clear output
- Average Risk 90%
- Graph values [11, 32, 42, 18]
Average Risk: 90%
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
Encrypted output
- Average Risk 3ca28a
- Graph Values ae4d729e
SecureView
upload
download
render
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Computation
Encrypted output
- Average Risk 3ca28a
- Graph Values ae4d729e


Bridge
Client App
Server
APIs
FHE APIs
Clear inputs
- Age 32 yo
- Weight 75kg
- Heartbeat 65 BPM
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Encryption
Client Key
Server Key
Enclave
Clear output
- Average Risk 90%
- Graph values [11, 32, 42, 18]
Average Risk: 90%
render
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
Encrypted output
- Average Risk 3ca28a
- Graph Values ae4d729e
SecureView
Average Risk: 90%
upload
download
Encrypted inputs
- Age bf8af50b
- Weight 21e00ab3
- Heartbeat 4b88957a
FHE Computation
Encrypted output
- Average Risk 3ca28a
- Graph Values ae4d729e

Demo

Conclusion

- TFHE-rs runs on iPhone (keygen + compute)
- Decryption can occur out-of-process (secure enclave)
- Code available at github.com/zama-ai/fhe_appstore_on_ios
- Feedback & contributions welcome:
  - Creating a real Server Part
  - Compelling use case & demo
  - TFHE-swift ? Better integration with Swift ecosystem