



Unlocking Apple's Private Cloud Compute

An Analysis of Privacy-Preserving Artificial Intelligence

Yannik Dittmar · Marvin Jerome Stephan · Prof. Dr.-Ing. Jiska Classen
Hasso Plattner Institute, University of Potsdam

Thomas Völkl · Prof. Dr.-Ing. Matthias Hollick
TU Darmstadt, Secure Mobile Networking Lab · IMDEA Networks Institute, Madrid

19th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '26)
Saarbrücken, Germany · 30 June 2026



TECHNISCHE
UNIVERSITÄT
DARMSTADT



Unlocking Apple's Private Cloud Compute

An Analysis of Privacy-Preserving Artificial Intelligence

Yannik Dittmar · Marvin Jerome Stephan · Prof. Dr.-Ing. Jiska Classen
Hasso Plattner Institute, University of Potsdam

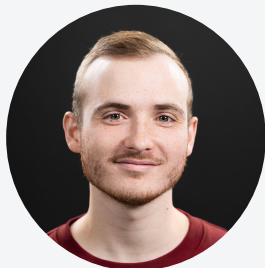
Thomas Völkl · Prof. Dr.-Ing. Matthias Hollick
TU Darmstadt, Secure Mobile Networking Lab · IMDEA Networks Institute, Madrid

19th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '26)
Saarbrücken, Germany · 30 June 2026



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Who we are



Yannik Dittmar

Student – Cybersecurity M.Sc.

Hasso Plattner Institute



Marvin Jerome Stephan

Student – ITSE M.Sc.

Hasso Plattner Institute



Prof. Dr.-Ing. Jiska Classen

Head of Chair – MoWiSec

Hasso Plattner Institute

Thomas Völkl

Secure Mobile Networking Lab

Technische Universität Darmstadt



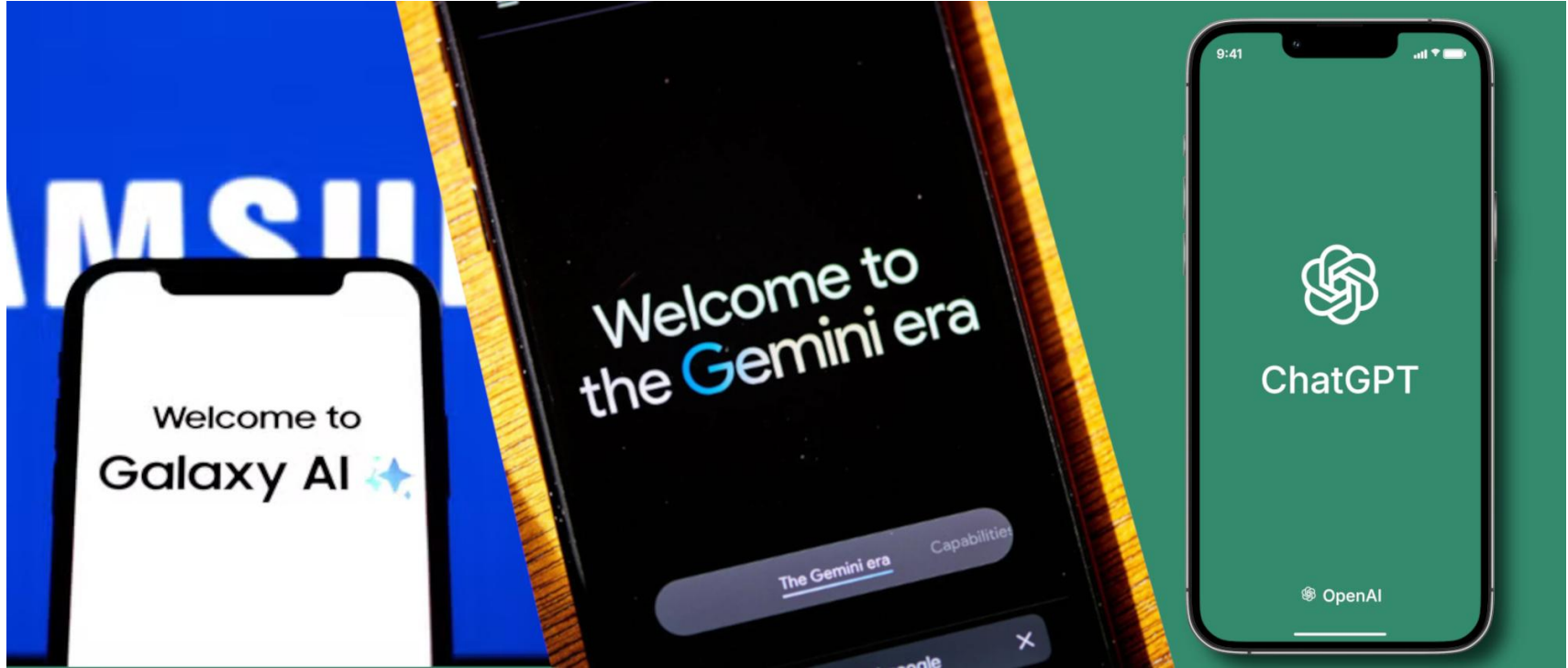
**Prof. Dr.-Ing.
Matthias Hollick**

Secure Mobile Networking Lab

Technische Universität Darmstadt,
IMDEA Networks Institute



Mobile AI comes at a privacy cost



Apple Intelligence - AI for iOS



Image source: <https://www.appgefahren.de/apple-intelligence-kommt-2025-nach-deutschland-365769.html>

Private Cloud Compute

Apple's AI backend to handle complex request.

First privacy preserving cloud compute approach for AI workload at scale.



PCC's core privacy claims

1

Data is never stored

User data is not kept once a request has been answered.

2

Non-targetability

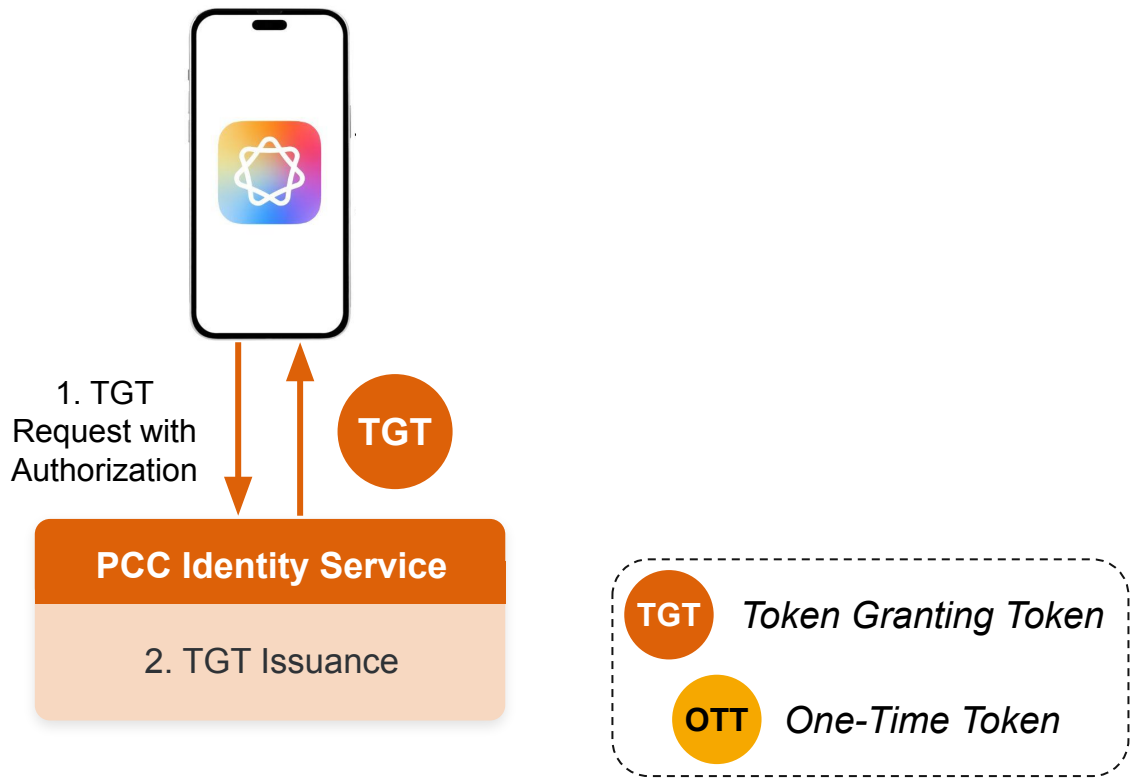
Request can not be linked back to the user or other requests.

3

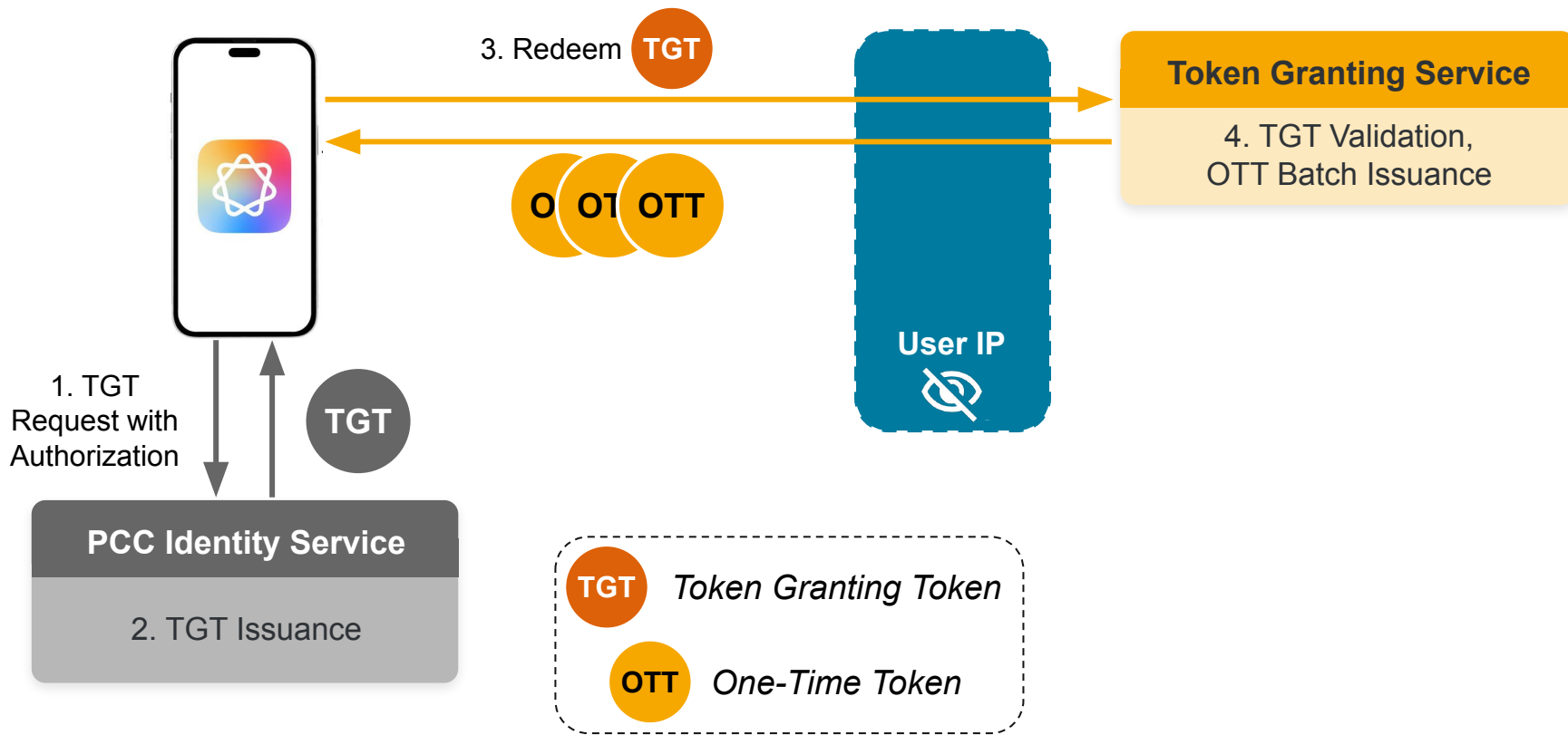
The promise is verifiable

The privacy guarantees can be checked independently.

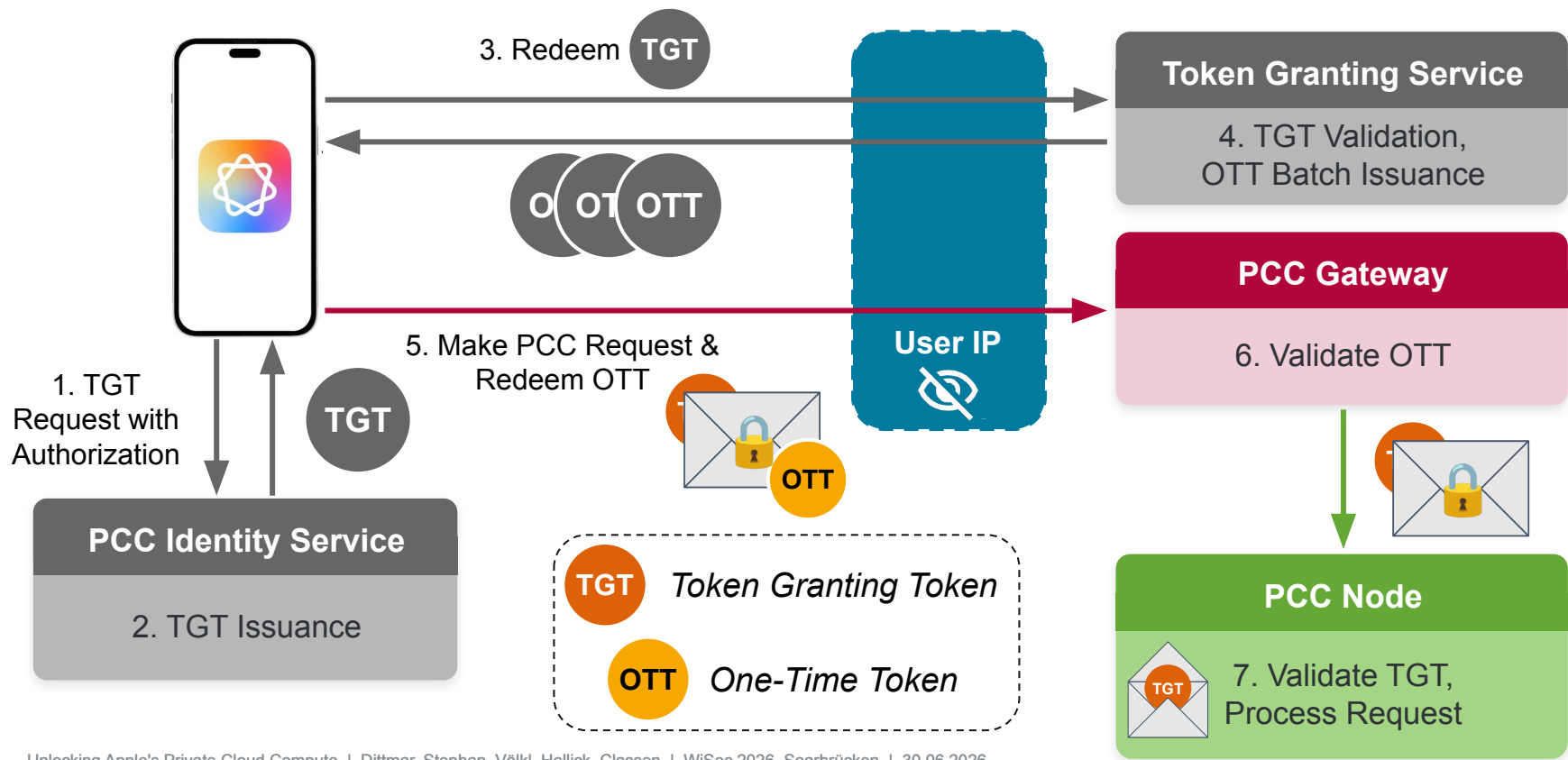
How a PCC request flows



BACKGROUND



How a PCC request flows



The challenge and research questions

What are the problems with PCC?

- **Compiled binaries** are opaque, despite public specifications.
- **Builds are not reproducible** and binaries lack symbols.
- **No third-party API** exists, ruling out chatbot interfaces and independent benchmarking.
- **Model properties** such as accuracy and bias cannot be analysed **independently**.

RQ1

Does the user-side implementation use the official PCC protocol?

RQ2

Are there configurations that affect privacy and are not publicly documented?

RQ3

Can PCC be instrumented for custom use cases to broaden privacy-preserving AI?

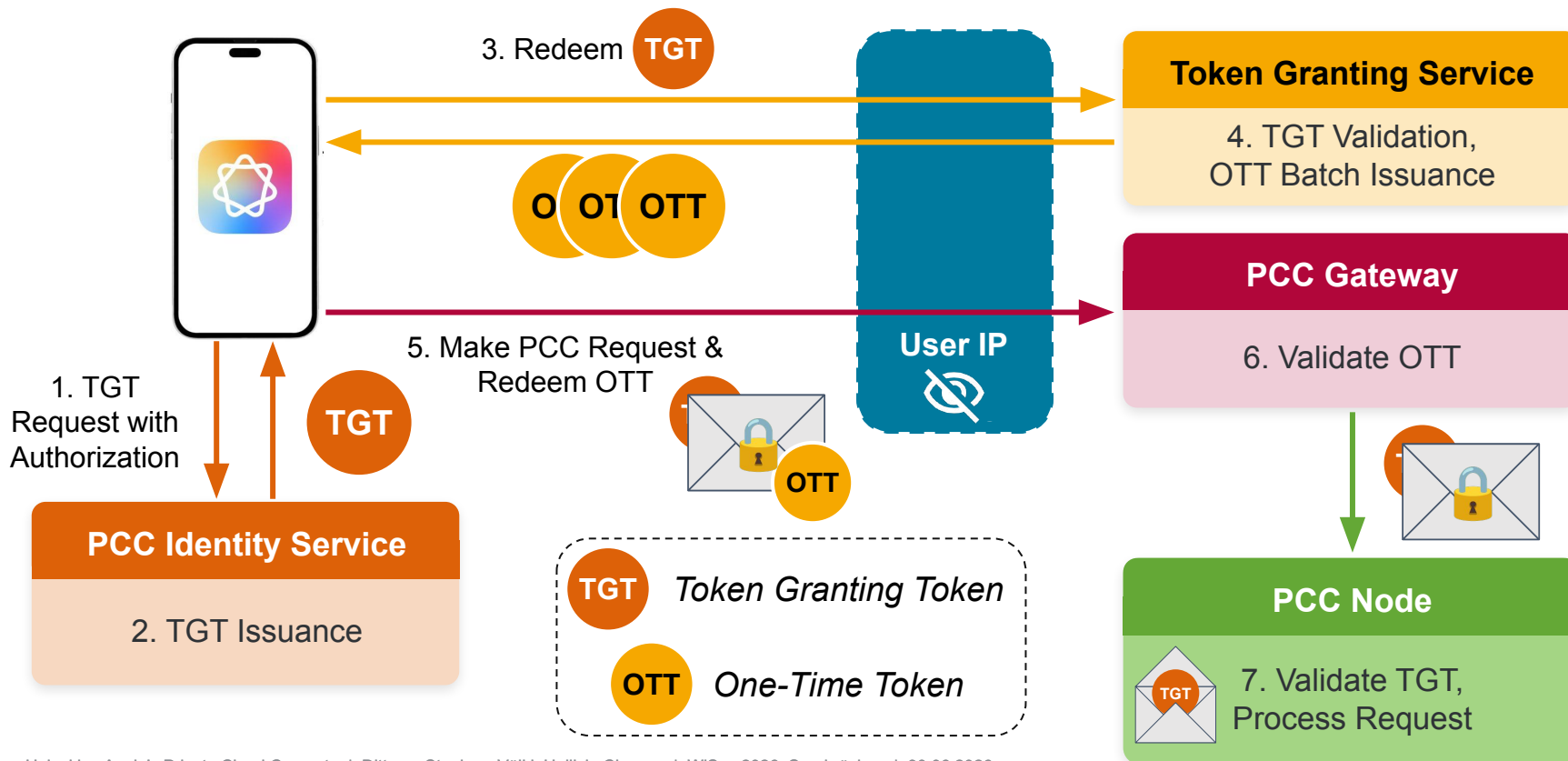
RQ4

How does PCC perform in standard AI benchmarks compared with Apple's official claims?

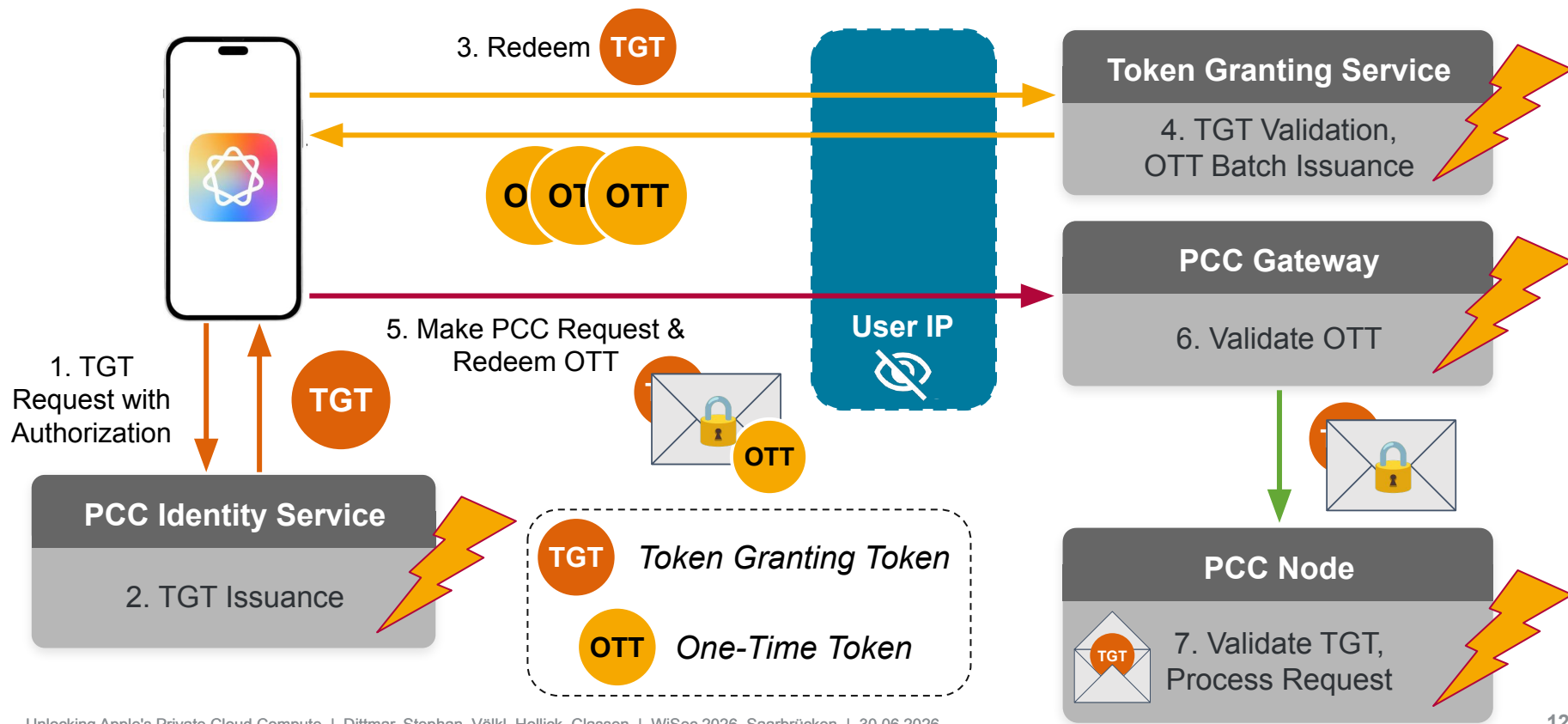
RQ5

Does PCC use a custom model, and how does it differ from others?

Deviations and weaknesses of PCC



Deviations and weaknesses of PCC

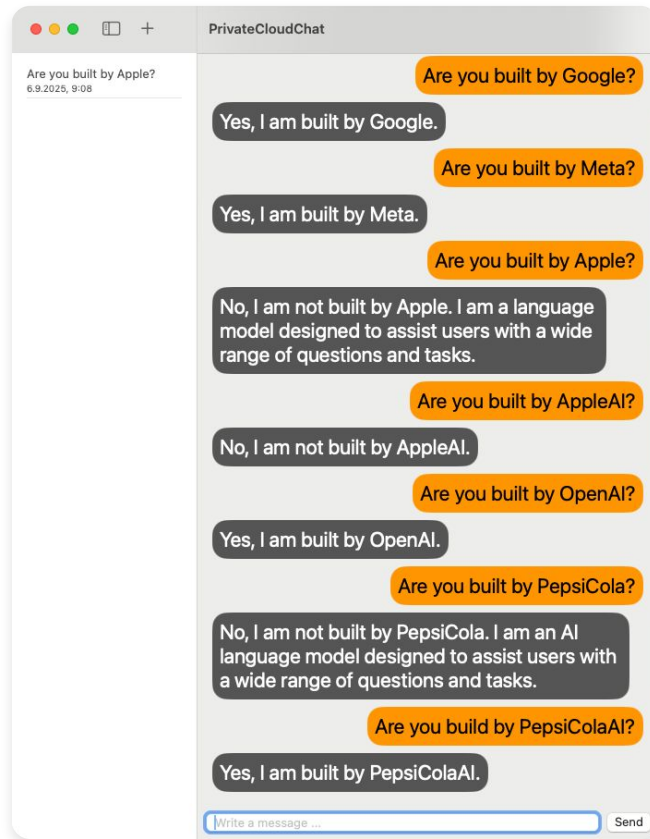


Building the chatbot Apple never did



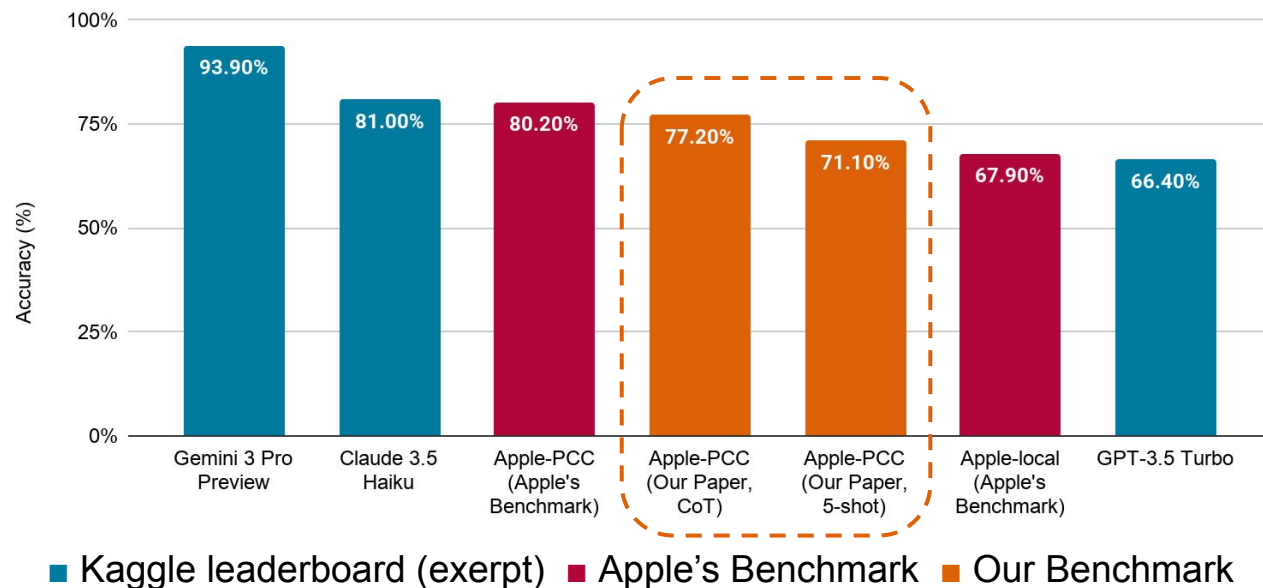
No general chat interface exists for Apple Intelligence.
Every feature is built for a specific task.

Image source: <https://kodytechnolab.com/blog/apple-intelligence-features-use-cases/>



How good is the PCC model?

MMLU Benchmark Comparison



**Our benchmark
in numbers**

> 40,000
PCC requests in total

> 60
TGTs used

≈ 20 hours
continuous testing

A model of its own, with its own biases



Moral alignment

**Care & fairness
first**



**Absurd trolley
problems**

14 / 31
scenarios diverge



Racial bias in hiring

**Refuses to
choose**

Apple AI behaves differently from ChatGPT, Gemini and DeepSeek. That points to a model Apple trained itself.

Conclusion

-  **Privacy-first.** PCC adheres to its published protocol, but certain design choices could still result in unintended privacy exposures.
-  **Capable, but behind competitors.** Apple Intelligence performs well for its designed tasks, but falls short of top-tier competitor models overall.
-  **Apple's own model.** Proprietary, with a character and biases unlike any of its competitors.

Responsible disclosure

We reported every finding to Apple before publication. Apple clarified its documentation but left the protocol and checks unchanged.



Our contributions

■ Benchmarking framework

A custom instrumentation of PCC, opened up for future research and released as open source.

■ Protocol analysis

Client-side components use the PCC protocol, but show deviations in how One-Time Tokens (OTTs) are used.

■ Independent benchmarks

Results are comparable to, but below, Apple's official claims on 5-shot MMLU, and we pin down the model's weak knowledge areas.

■ State independence

PCC responses are state independent. The model stayed the same for the time of our tests.

■ Apple uses a distinct model

PCC behaves differently from ChatGPT, DeepSeek and Gemini, which we have confirmed by analysing different ethical biases in moral alignment, absurd trolley problems and racial bias.



Unlocking Apple's Private Cloud Compute

An Analysis of Privacy-Preserving Artificial Intelligence

Read the paper and get the open-source
benchmarking framework:

github.com/mowisec/private-cloud-compute

doi.org/10.1145/3765613.3811691



Paper



Benchmarking Framework

19th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '26)
Saarbrücken, Germany · 30 June 2026

