WhatsKey-Trasparency

La crittografia dietro l’app di messagistica più famosa al mondo

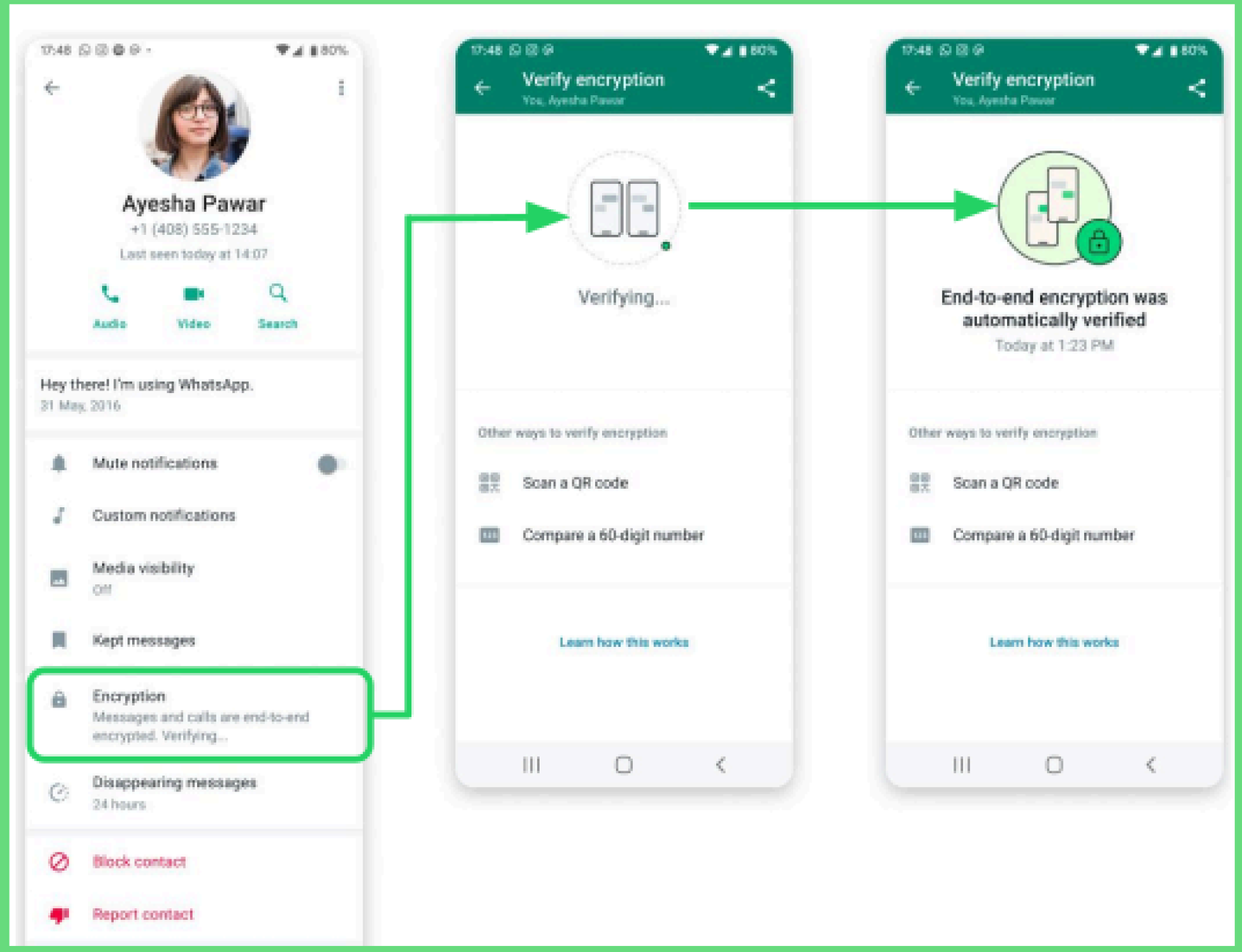
Salvatore Bianco, mat. 189353 , Crittografia Applicata 2024

Index

ARGUMENTS:

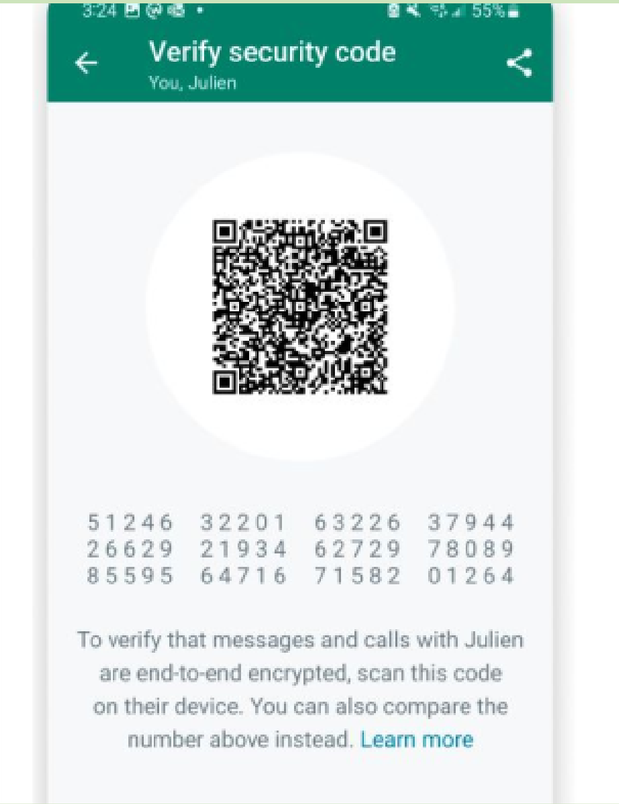
- Overview
- Infrastructure
- Auditable
- Demo

New cryptographic security feature



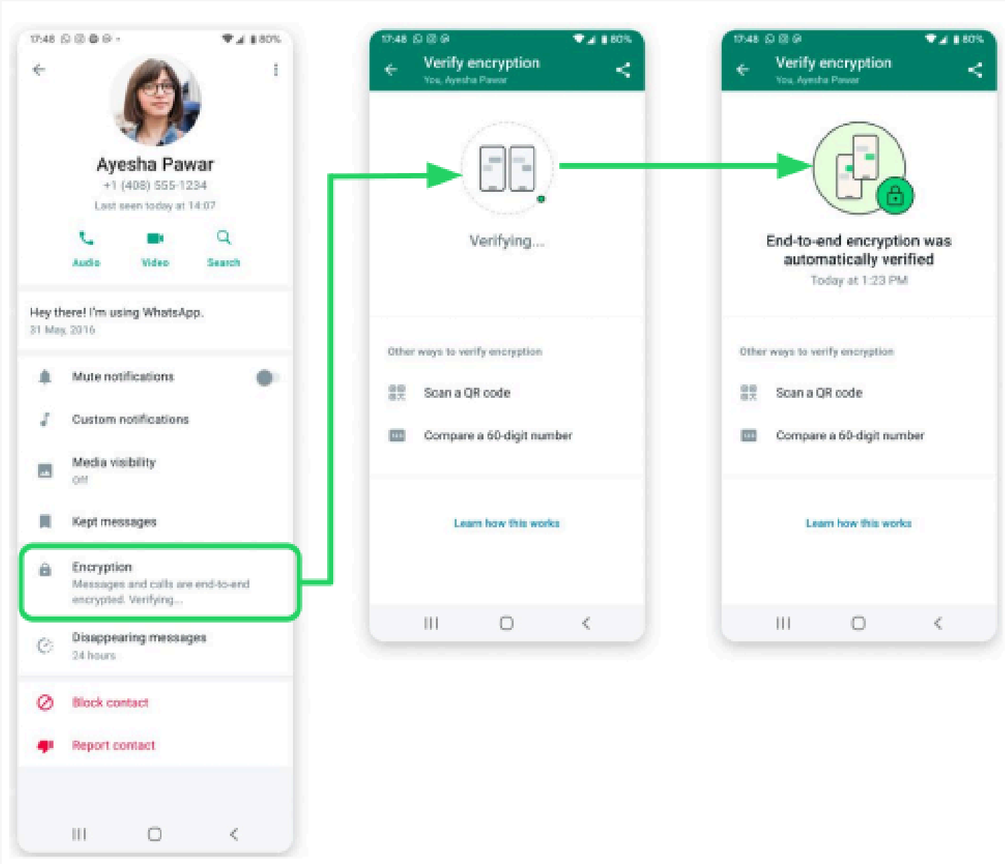
How did it work?

- Physically verification

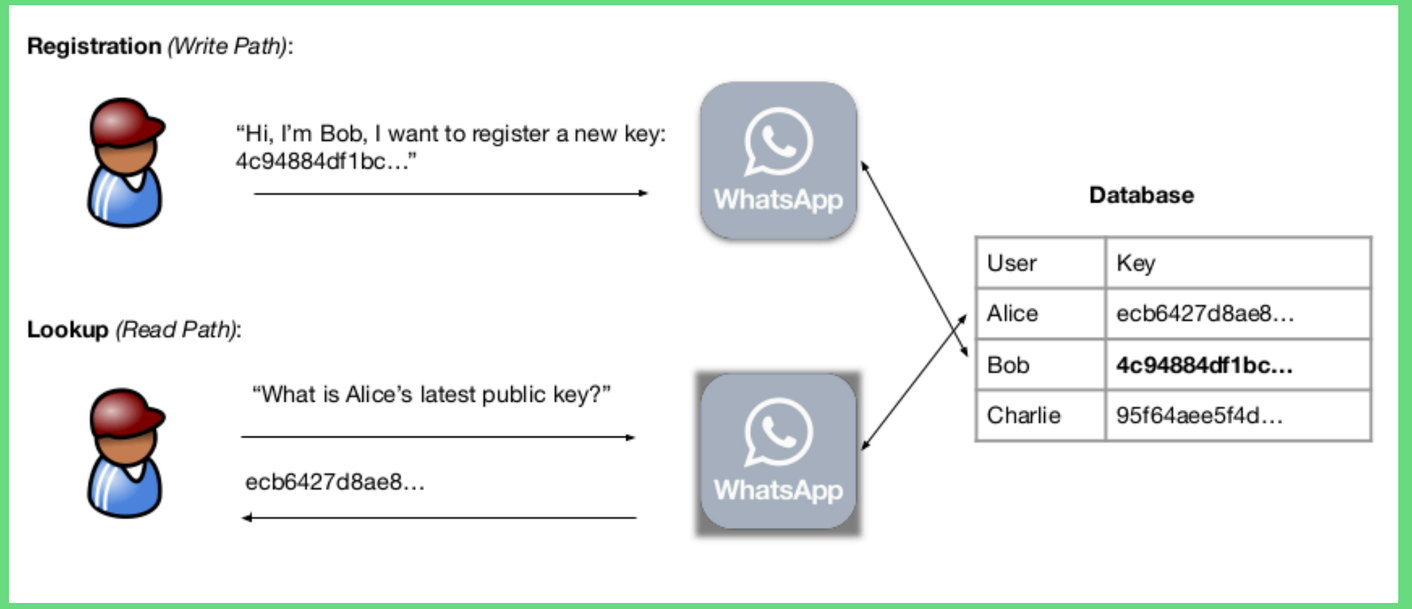


How does it work?

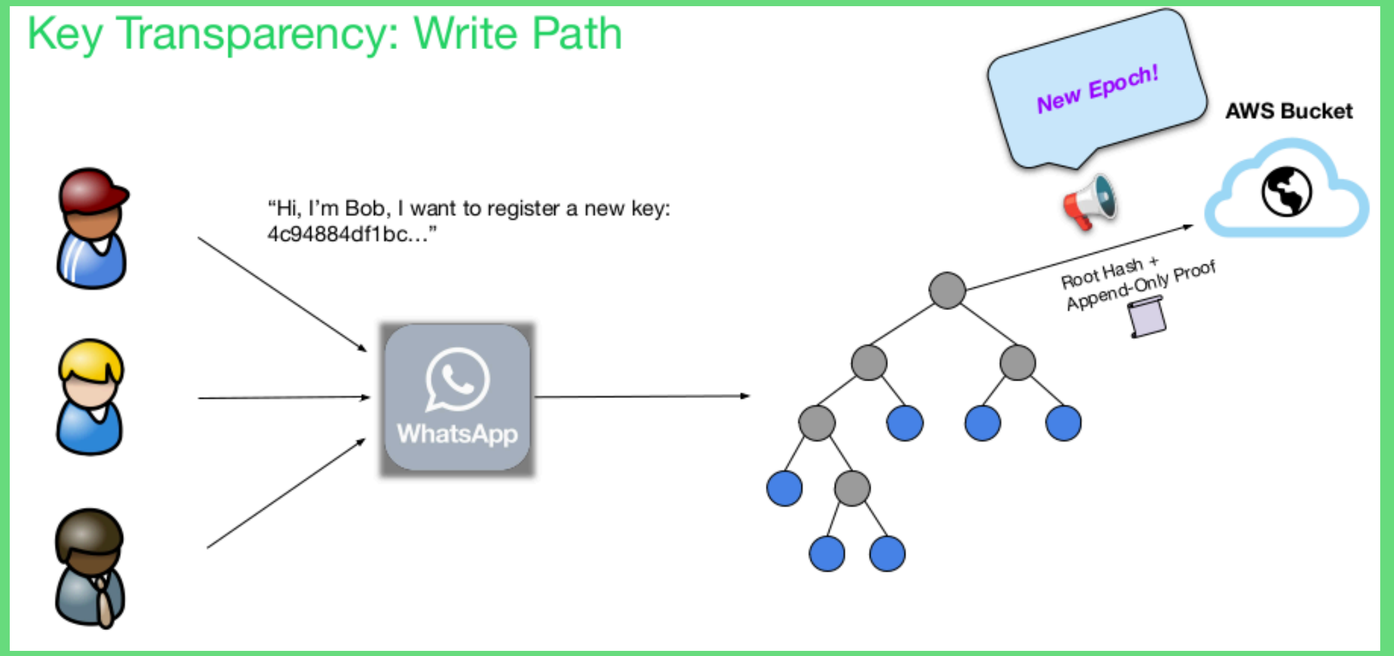
- Automatic validation of public keys



How did it work vs How does it work

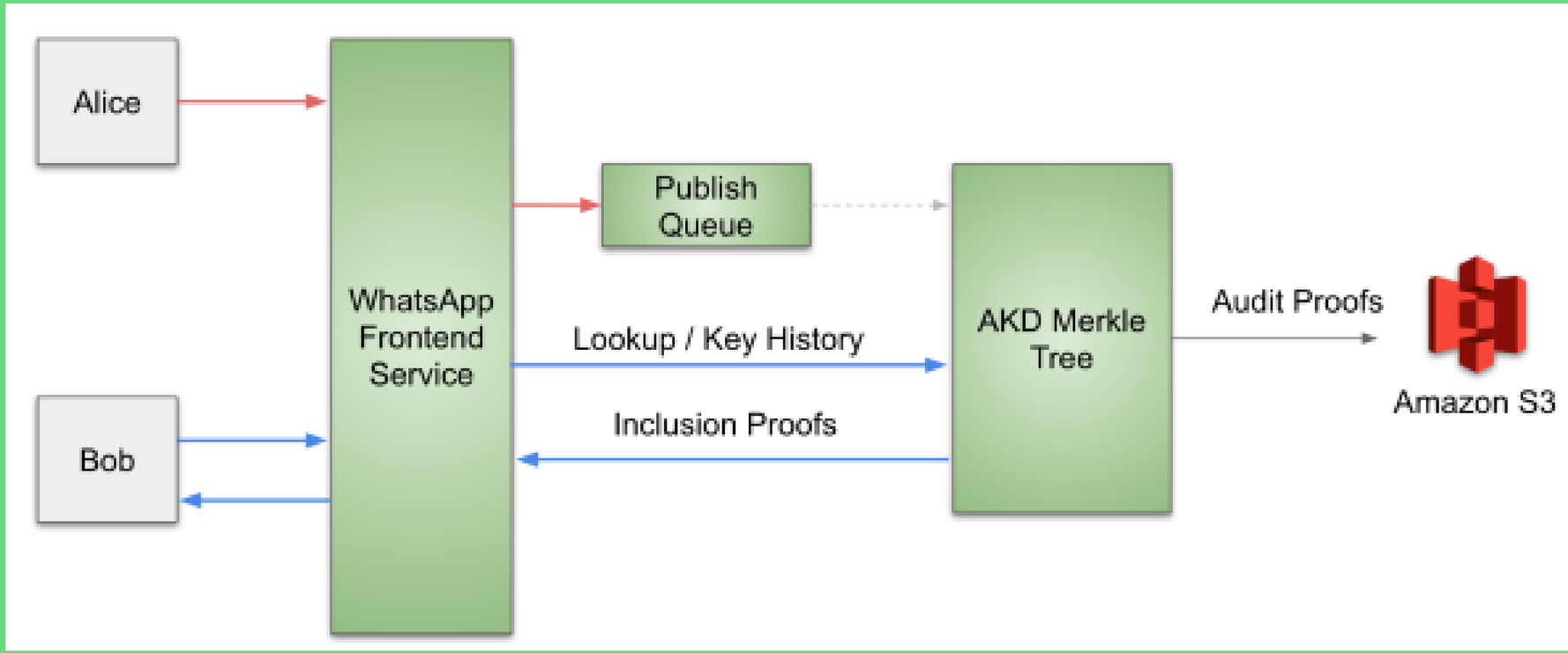


vs

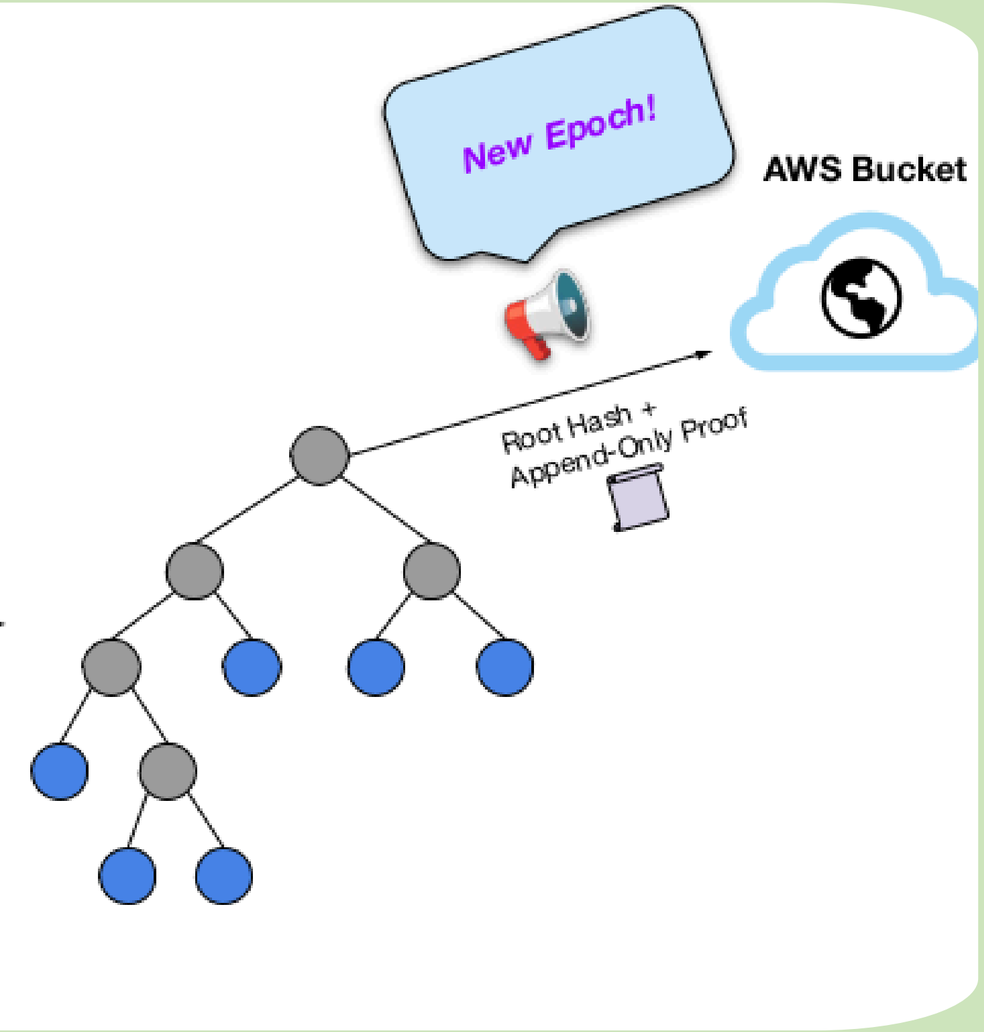


INFRASTRUCTURE

- Registration
  - Pubkey-Curve25519
- Lookup



More details

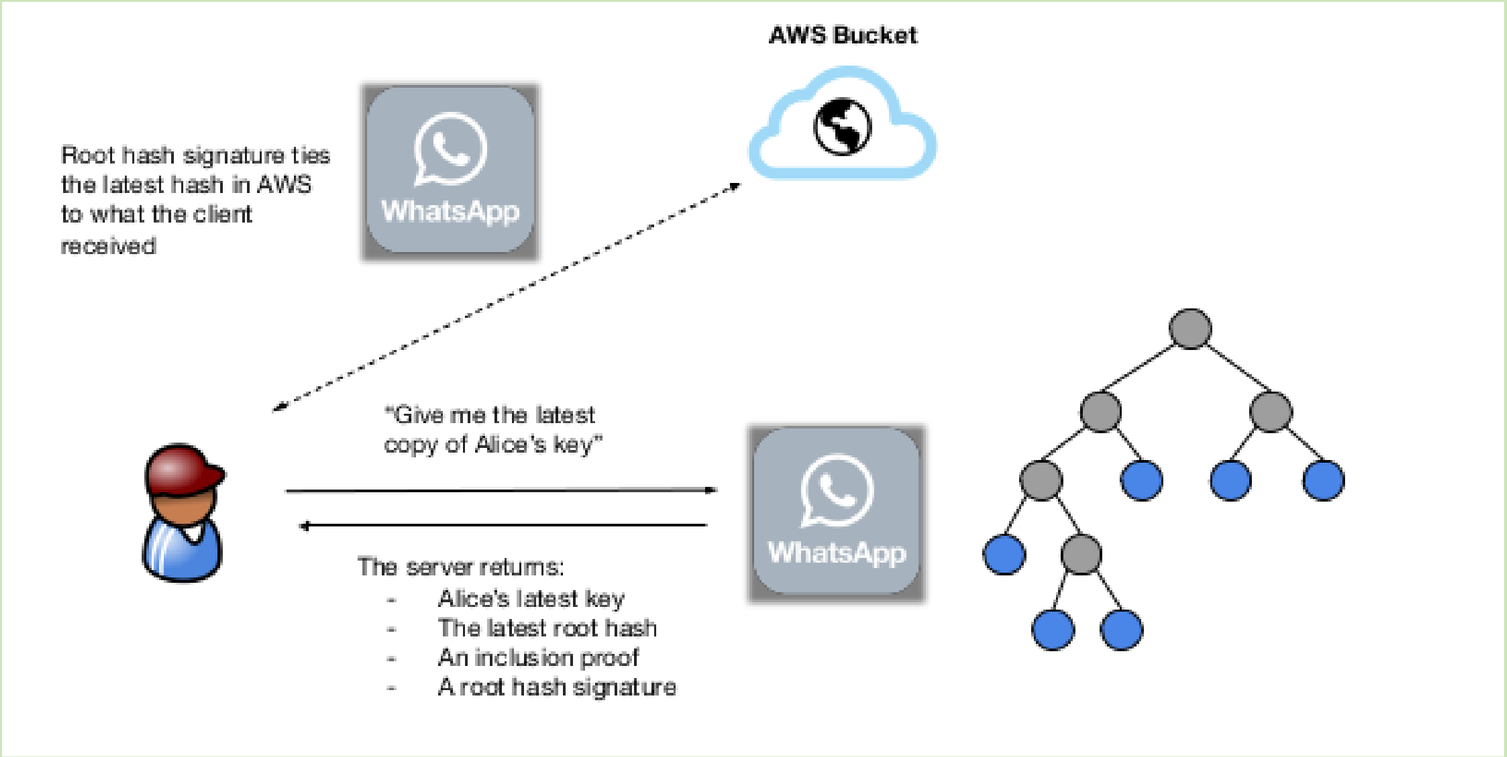


- Client Registration
  - Merkle tree
    - Hash function Blake3
  - VRF
  - Epoch
- Device Removal

How does lookup work?

Lookup Requests

- Client
- Server



Auditing

AUDIT AND FUTURE GOAL

01 Audit

- Proof
- AKD

02 Future goal

- Consistent root hash distribution
- Key history check

AKD

Auditable key directory

META AKD

- Publishing
- Lookup proofs
- History proofs
- Append only proofs

DEMO TIME!

- Language : Rust
- Crate: Meta Akd

xerox0/ WhatsKey-Transparency

References

1.WhatsApp Encryption Overview - technical white paper

https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

2.About end-to-end encryption - Help center article

https://faq.whatsapp.com/820124435853543

3.About security-code change notifications - Help center article

https://faq.whatsapp.com/1524220618005378

4.Auditable key directory (AKD) implementation

https://github.com/facebook/akd

Questions?

Just ask! I hope you have learned something new..