# Network Tokens: a mechanism for endpoint<>network coordination


Yiannis Yiakoumis, Co-Founder & CEO, Selfie Networks
yiannis@selfienetworks.com | https://networktokens.org

Joint work with Nick McKeown (Stanford University) and Frode Sorensen (Norwegian Telecommunications Authority)

# Two conflicting trends in networking

Networks become more capable and programmable

P4

eBPF

SDN

Virtualization

Network Slicing

5G

QoS

Analytics

Networks have less and less context about the traffic they carry

Cloud deployments

Third-party traffic

Rapidly-changing infrastructure

Privacy

Net Neutrality

DNS over HTTPS

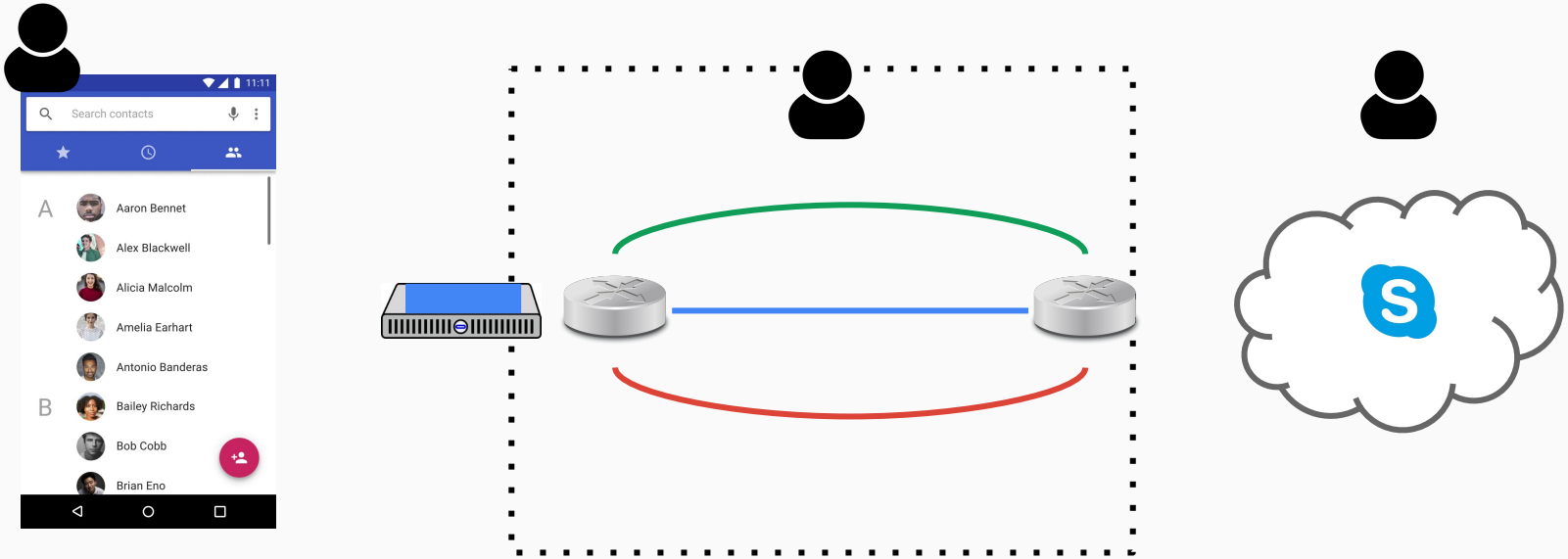
Encryption

Conventional wisdom) requires **“traffic classification”** (aka DPI) or **“insecure low-level mechanisms”** to map a high-level policy (e.g., “low latency for Skype”) to a network behavior. It is expensive (cost and performance), insecure, doesn’t scale, doesn’t work with upcoming encryption, and can’t support business and compliance requirements.

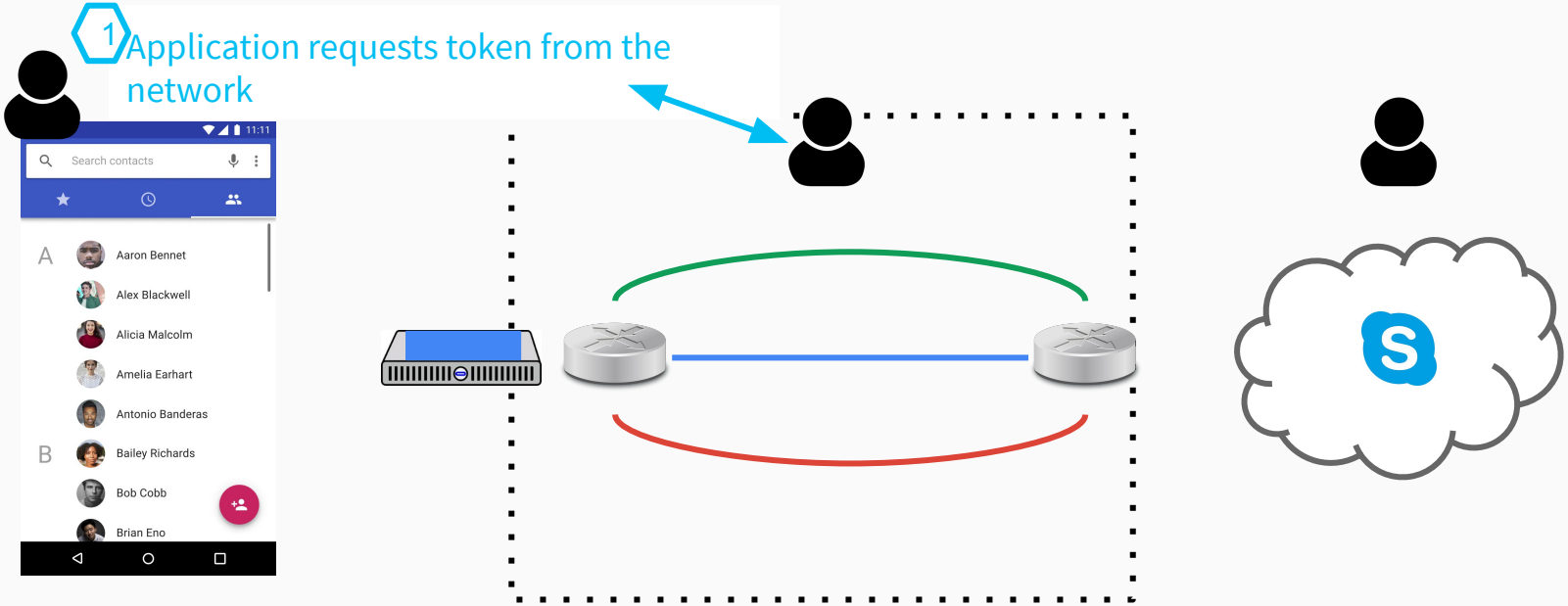
# How to move forward

**Network Tokens**: An explicit and secure mechanism for endpoints to coordinate with the network

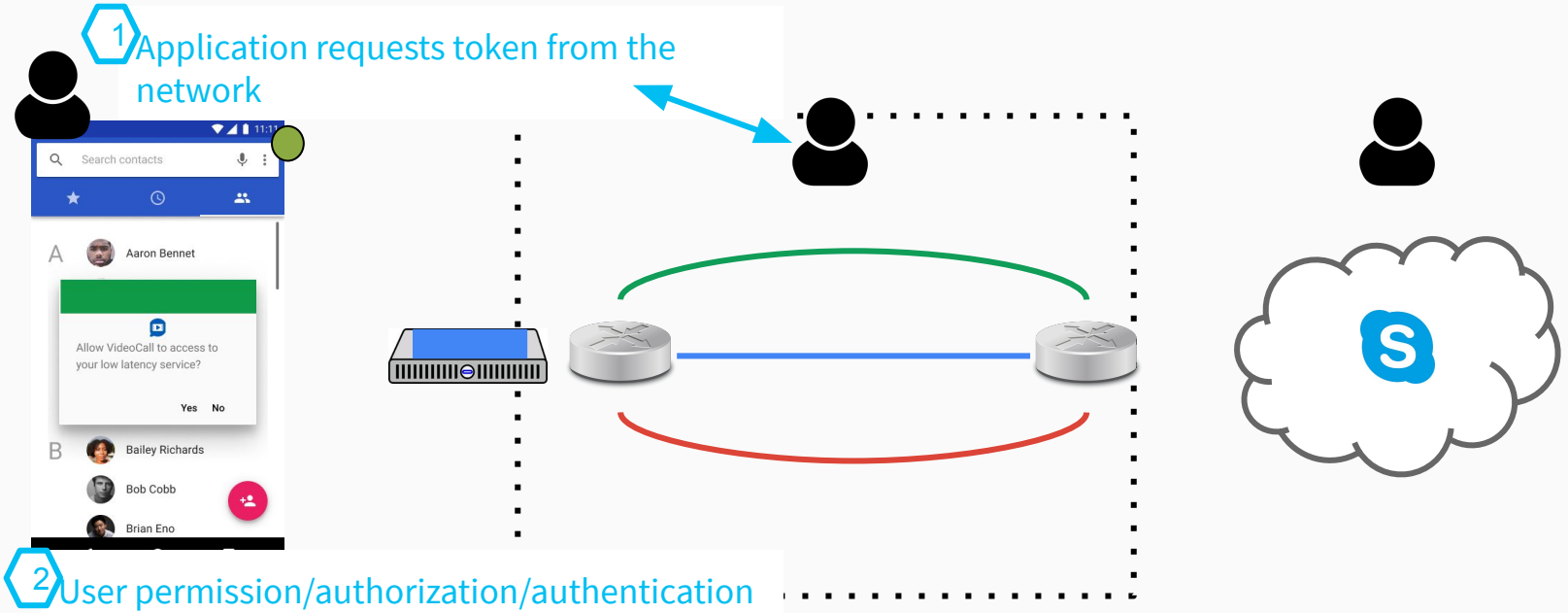
# How network tokens work



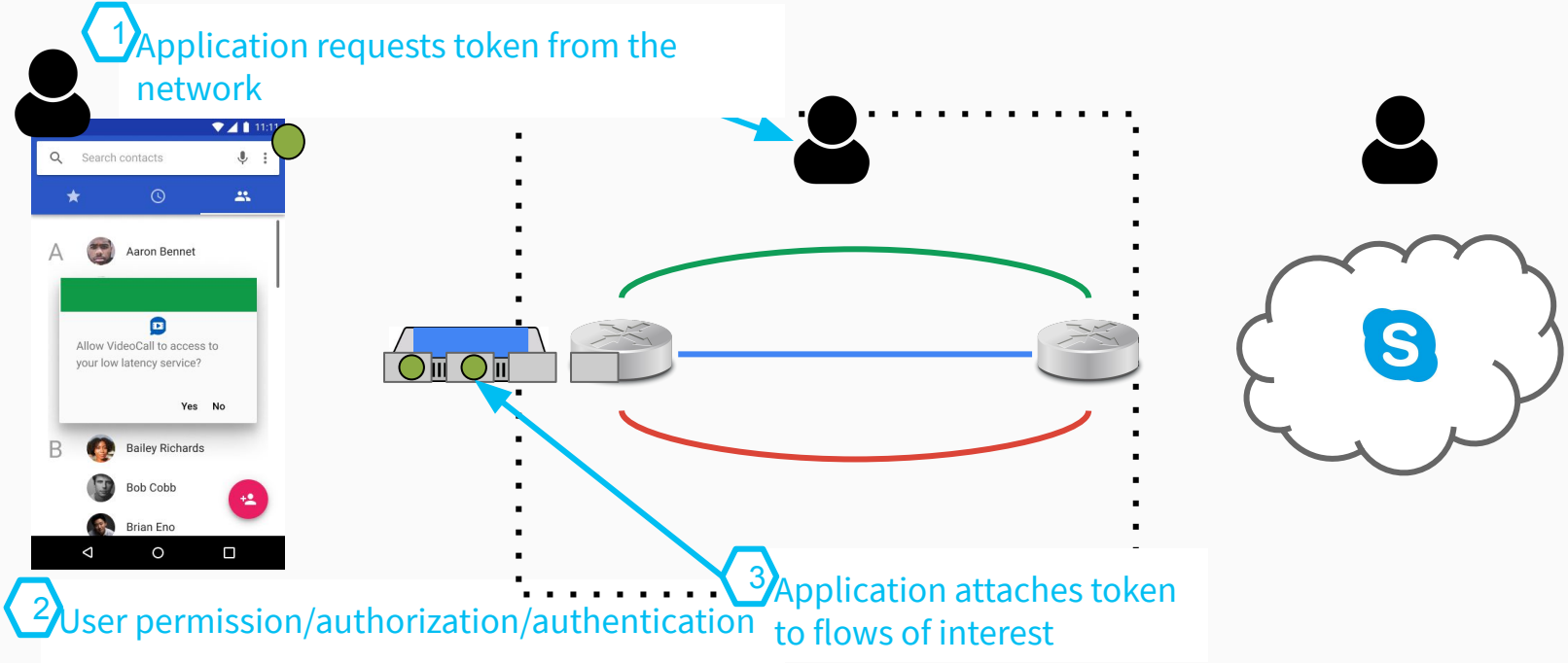
# How network tokens work



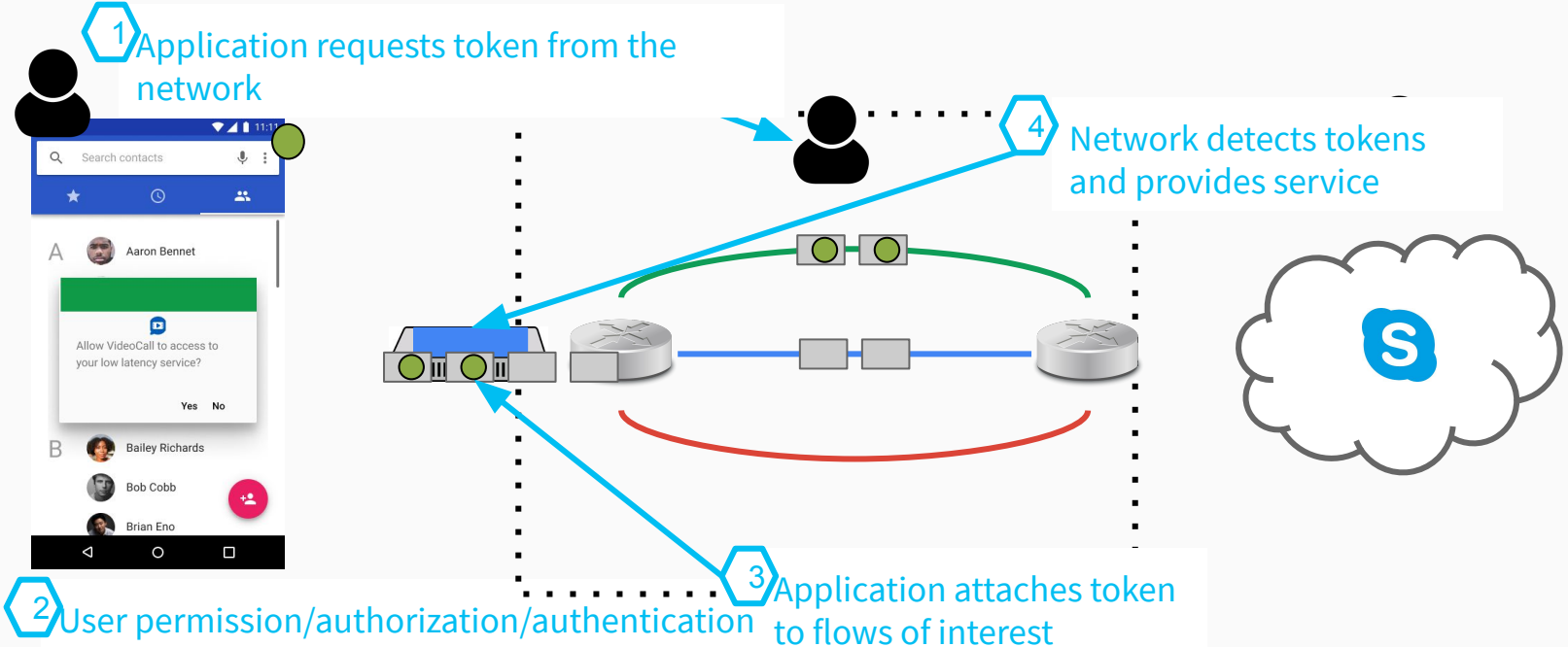
# How network tokens work



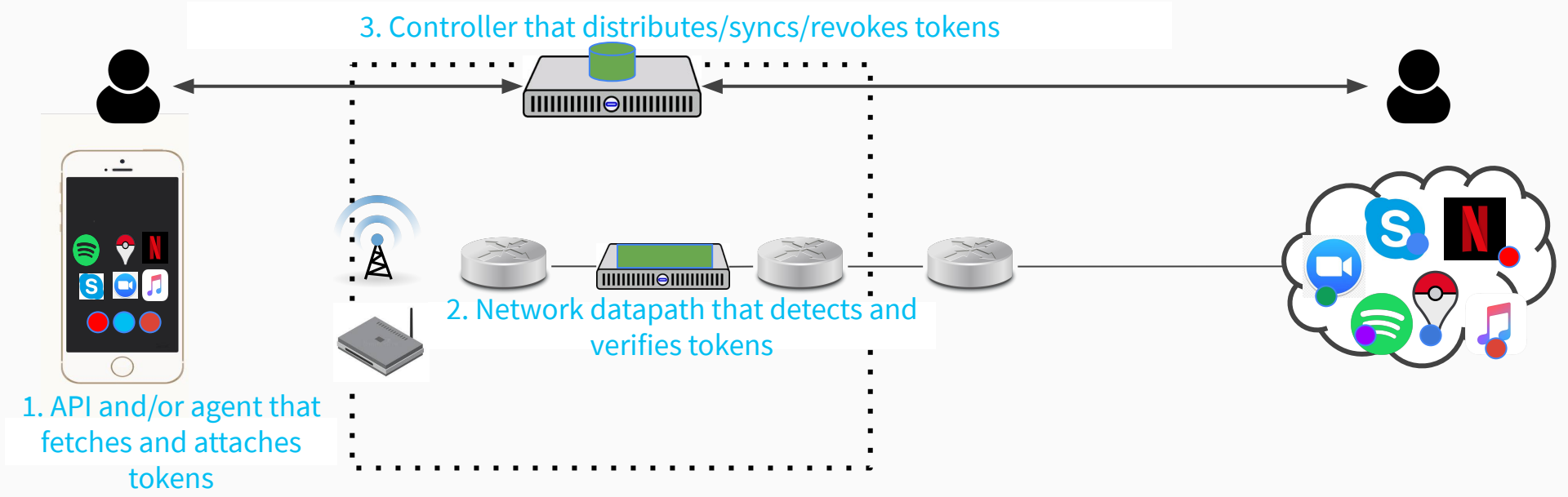
# How network tokens work



# How network tokens work



# Network Tokens Architecture

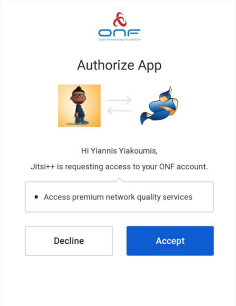


# Network Tokens

- Tokens carry simple claims (e.g., *“I am Skype”*, *“I need low latency”*)
- Encrypted and/or signed based on trust relationships and requirements
- Provisions against replay and spoofing attacks (expiration, binding, revocation)
- Represented as JWT, CWT, Custom Formats
- Inserted as extensions/attributes in existing protocols (e.g. IPv6, TLS, STUN)

# Status & Traction

**Open Specs, and IETF I-D for Network Tokens & Workflows**




**User-Centric + Application agnostic QoS implementation for LTE/5G**

**Running code for client API + network capabilities**

**https://networktokens.org**


# Thank you

yiannis@selfienetworks.com / LinkedIn / @gyiakoumis / https://networktokens.org