

Network Tokens

IETF 108, TSV Open Meeting, July 29th 2020

Yiannis Yiakoumis, Co-Founder & CEO, Selfie Networks

Work with Nick McKeown (Stanford), Frode Sorensen (NKOM), Tom Herbert (Intel)

<https://networktokens.org> | network-tokens@ietf.org | yiannis@selfienetworks.com

The good: Traffic Differentiation is...

- » Widely deployed worldwide (zero-rating, firewall whitelists, QoS)
- » Can improve user experience
- » Can help operators monetize their infrastructure

The bad: Traffic ↔ Service Mapping is...

- » Primarily done through traffic classification (app signatures, DPI, ...)
- » High implementation/operational overhead for everyone
- » In conflict with user privacy and encryption (e.g., tls-esni)

The ugly: unclear who controls what traffic gets differentiated...

- » User? Network Operator? App provider? OS? DPI Vendor?

Can we do any better?

How can we expose and access traffic differentiation services in a way that ...

1. is easy for operators to deploy and operate
2. is easy for end-users and app providers to access
3. respects user privacy and user choice
4. works with encryption and modern infrastructure (ESNI, multi-cloud, 3rd-party APIs)

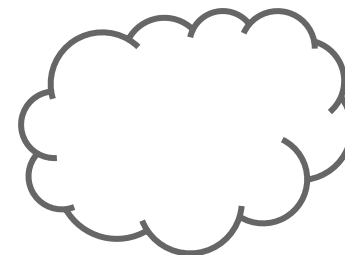
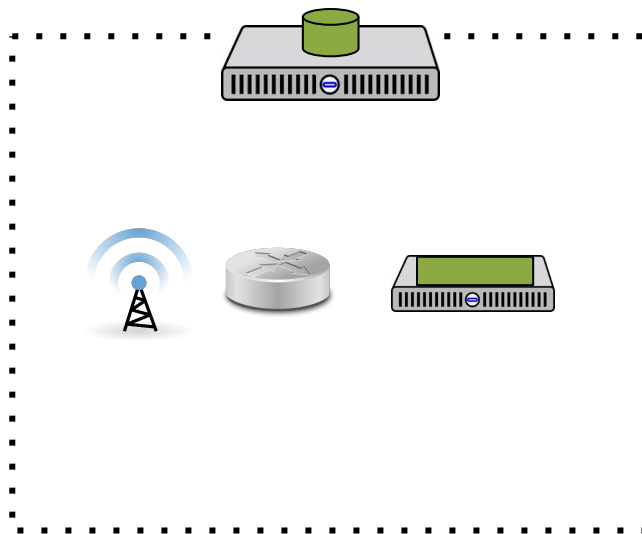
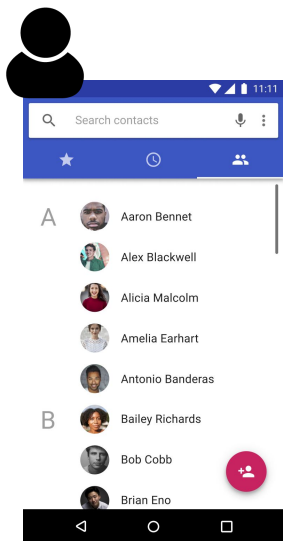
- » Explicit and secure coordination between end-users/apps and the network
- » They replace heuristics and application signatures/DPI with deterministic mechanism
- » Heavily influenced by Json Web Tokens (JWT), access tokens, and OAUTH2 workflows

- 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)

Tokens are policy agnostic. Policy dictated by token distribution, crypto functions, E2E workflows

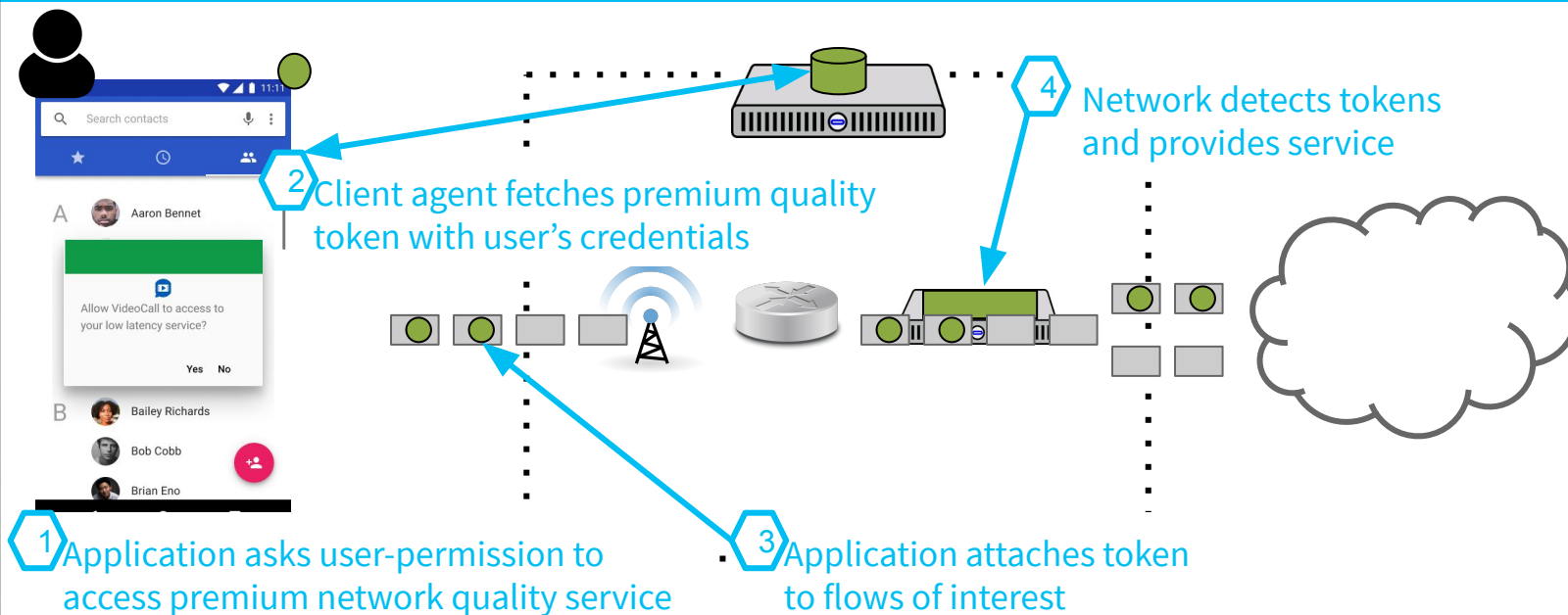
- User-centric, application agnostic token (e.g. for QoS service)
- App-specific token (e.g., firewall whitelist, zero-rating)

Sample workflow: user-centric, application-agnostic tokens



Sample workflow: user-centric, application-agnostic tokens

8



Current Status

- » Network Tokens I-D (draft-yiakoumis-network-tokens-01)
- » Mailing List at network-tokens@ietf.org
- » Blueprint implementation
 - » User-centric tokens + 4G/5G QoS + WebRTC/STUN (Open-source @ ONF)

Next Steps

- » Engage with related groups (TLS, IPv6, WebRTC)
- » Prioritize specific use case
- » Where to host this work
- » Work towards BoF for IETF 109/110

- » network-tokens@ietf.org | <https://networktokens.org>
- » Network Token Side Meeting: Thursday 07/30 @ 4pm UTC
- » APN Side Meeting : Thursday 07/30 @ 12:30pm UTC

Thank you!

yiannis@selfienetworks.com

Appendix

Design Priorities

- » Deal with privacy, security, roles
- » Path to adoption
- » Implementation efficiency

Trade-off considerations

- » Per-packet/Per-flow ? Opaque/Structured tokens?
- » L3 or Transport?
- » What is the role of the OS?

Tokens are policy agnostic. Policy dictated by token distribution and crypto functions

App-specific token

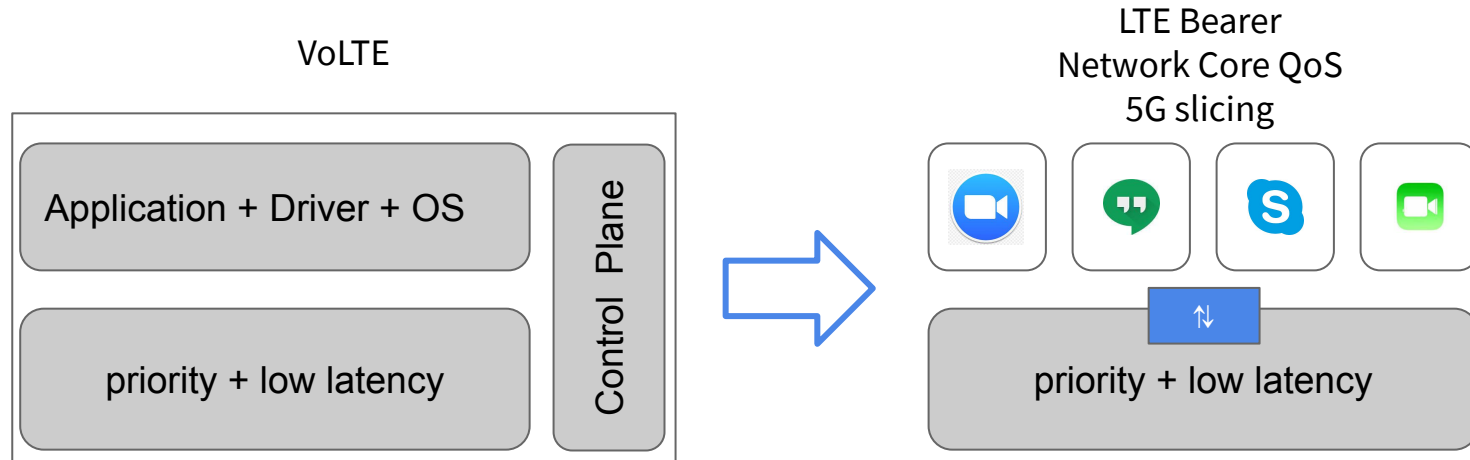
```
{"alg": "ES256", "kid": "N6fr1MDrEuu1eXRkFbcpX4WY62SKN7TKrhYf9PfJEd8"}. {"sub": "Skype",  
"iat": 1588116732, "exp": 1588117732, "bip": "140.54.35.194"}
```

User-driven, application agnostic, privacy aware token

```
{'alg': 'dir', 'app id': 'low-latency'}. {'sub': '+14151234567', 'nti':  
5871234, 'exp': 1588203132}
```

Opening-up existing QoS services with tokens

14



- IETF: Network tokens as interface between network and apps/end-users
- 3GPP : How do network tokens fit in 3GPP architecture?
 - Most functionality fits under existing TDF/DPI interfaces (Gy, Gw, Sd, ...)
 - Adding tokens to packet filters & traffic-flow-templates can help