

Proof of Transit

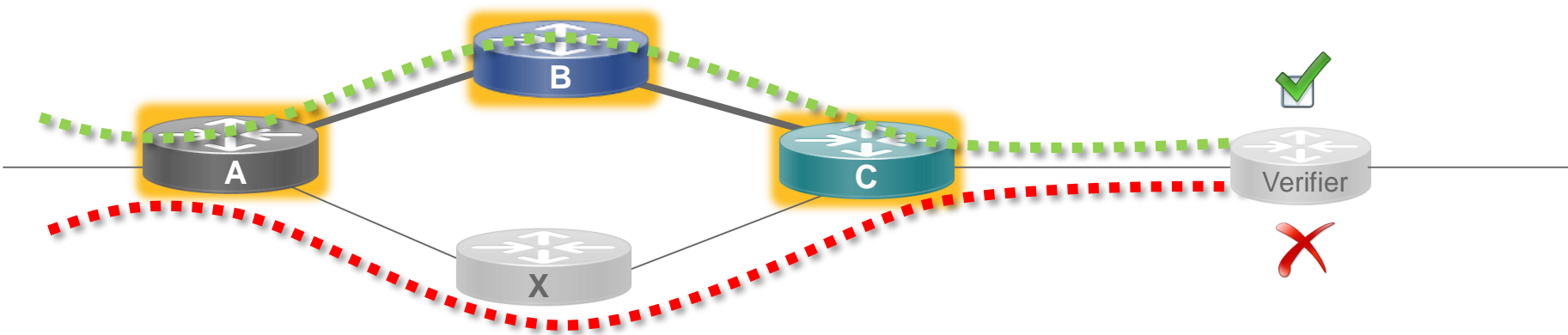
Frank Brockners, Shwetha Bhandari,
Sashank Dara, Carlos Pignataro (Cisco)
Hannes Gedler (rtbrick)
Steve Youell (JMPC)
John Leddy (Comcast)
David Mozes (Mellanox Technologies)
Tal Mizrahi (Marvell)

IETF 101 London – SFC WG; March 21, 2018

[draft-brockners-proof-of-transit-04](#)

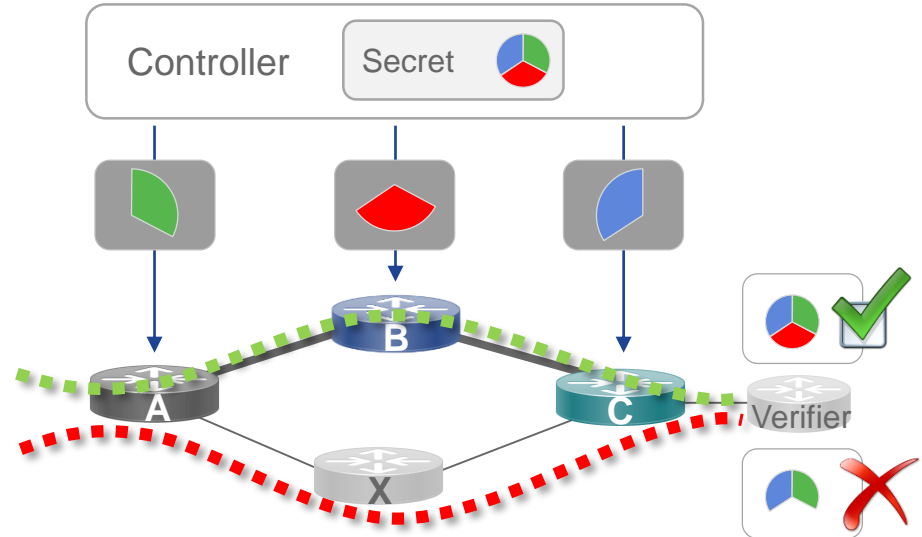
Consider TE, Service Chaining, Policy Based Routing, etc...

“How do you *prove* that traffic follows the selected path?”

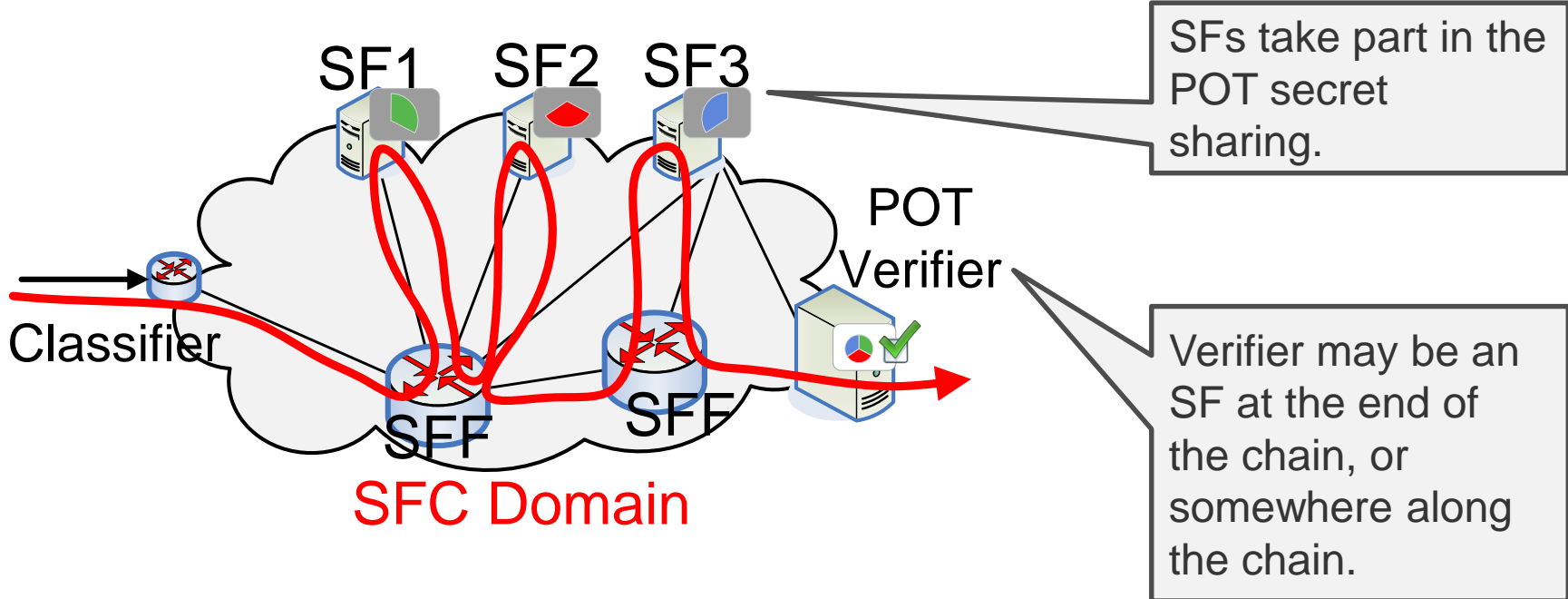


Ensuring Path and/or Service Chain Integrity Approach

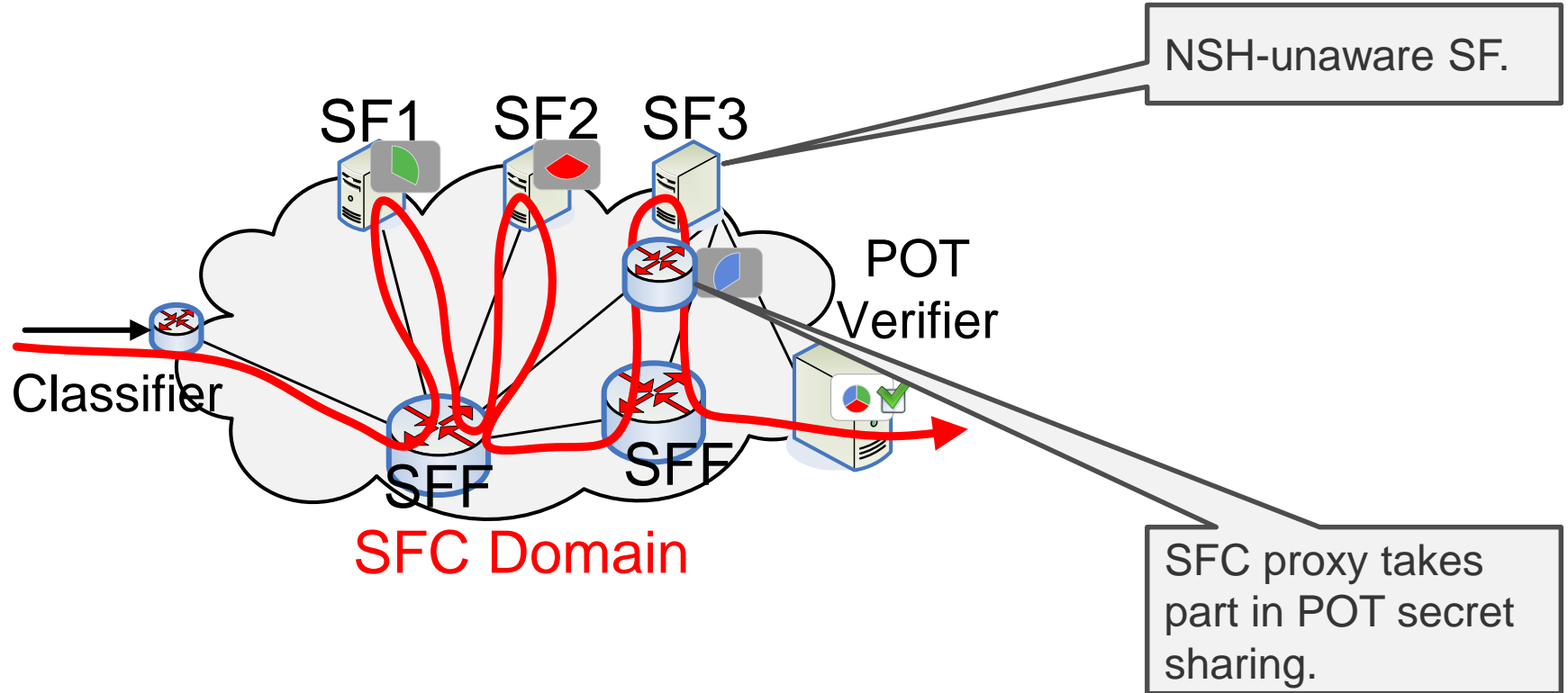
- Meta-data added to all user traffic
 - Based on “Share of a secret”
 - Provisioned by controller over secure channel to hops where “proof of transit” is required
 - Updated at every hop where proof of transit is required
- Verifier checks whether collected meta-data allows retrieval of secret
 - ➡ “Proof of Transit”: Path verified



POT in an SFC Domain



POT in an SFC Domain with SFC Proxy



So what has changed?

The draft has not changed significantly since version 03.

However, new SFC charter:

"...Security and Privacy - Mechanisms and guidance for securing metadata via authentication, integrity protection, confidentiality, and/or data minimization are not yet defined. What can be effectively provided, for which scenarios, and how those tools can be provided need to be determined and the tools standardized..."

Next Steps

- POT concept (and associated draft) has been presented 3 times in SFC WG.
RFC 8300 already references POT.
Security and Privacy are now part of the charter.
- WG adoption call