Signposts

Signposts provides users with a secure, simple mechanism to establish and maintain communication channels between their personal cloud of named devices. Signpost names exist in the DNSSEC hierarchy, and resolve to secure end-points when accessed by existing DNS clients.

Signpost clients intercept user connection intentions while adding privacy and multipath support. Signpost servers co-ordinate clients to dynamically discover routes and overcome the middleboxes that pervade modern edge networks.

Middlebox traversal

Using a tactics engine, Signposts automatically traverses the middleboxes between your devices.

Multipath

Signposts allows processes to transparently communicate using multipath TCP.

Secure identity

Signposts is built on top of DNSSEC. DNSSEC gives both the connecting device, and the device being connected to, a verifiable identity. DNSSEC is also used to derive secrets (e.g., PEM or X.509) for initiating encrypted communication between devices.

Andrius Aucinas, Jon Crowcroft, Sebastian Probst Eide, Steve Hand, Anil Madhavapeddy, Andrew W. Moore, Richard Mortier, Haris Rotsos, and Narseo Vallina-Rodriguez