CLOUDFLARE

Auditing Key Transparency

With a live demo from Transparency.dev summit

Thibault Meunier
Research Engineer

Multiple papers and deployment

CONIKS: Bringing Key Transparency to End Users

Marcela S. Melara and Aaron Blankstein, *Princeton University;* Joseph Bonneau, *Stanford University and The Electronic Frontier Foundation;* Edward W. Felten and Michael J. Freedman, *Princeton University*

https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/melara

SEEM*less*: Secure End-to-End Encrypted Messaging with *less* Trust

Parakeet: Practical Key Transparency for End-to-End Encrypted Messaging

Harjasleen Malvai*†, Lefteris Kokoris-Kogias‡§, Alberto Sonnino‡¶, Esha Ghosh‖, Ercan Oztürk**, Kevin Lewi**, and Sean Lawlor**
*UIUC, †IC3, ‡Mysten Labs, §IST Austria, ¶University College London (UCL), ‖Microsoft Research, **Meta

OPTIKS: An Optimized Key Transparency System

Julia Len, *Cornell Tech;* Melissa Chase, Esha Ghosh, Kim Laine, and Radames Cruz Moreno, *Microsoft Research*

https://www.usenix.org/conference/usenixsecurity24/presentation/len

ELEKTRA: Efficient Lightweight multi-dEvice Key TRAnsparency*

Julia Len†
Cornell Tech
New York, USA
jlen@cs.cornell.edu

Melissa Chase
Microsoft Research
Redmond, USA
melissac@microsoft.com

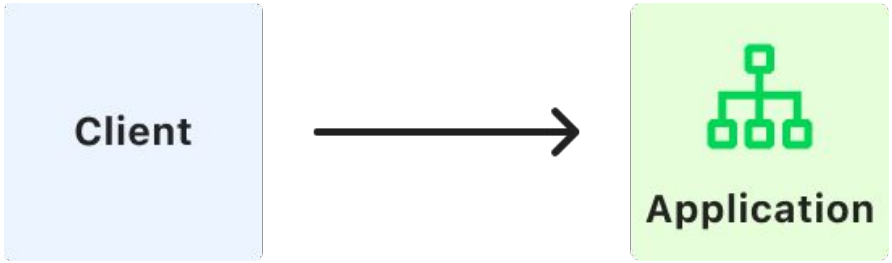
Esha Ghosh
Microsoft Research
Redmond, USA
esha.ghosh@microsoft.com

Daniel Jost
New York University
New York, USA
daniel.jost@cs.nyu.edu

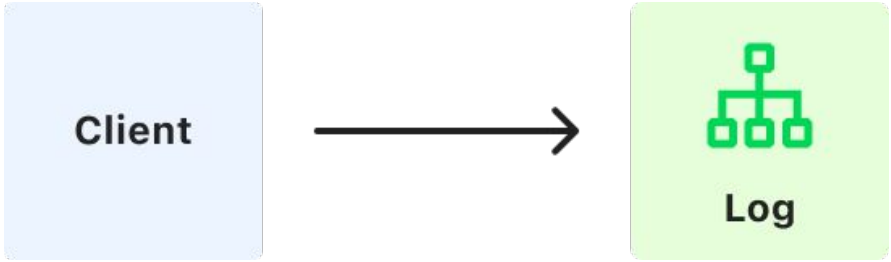
Balachandar Kesavan
Zoom Video Communications
New York, USA
surya.heronhaye@zoom.us

Antonio Marcedone
Zoom Video Communications
New York, USA
antonio.marcedone@zoom.us

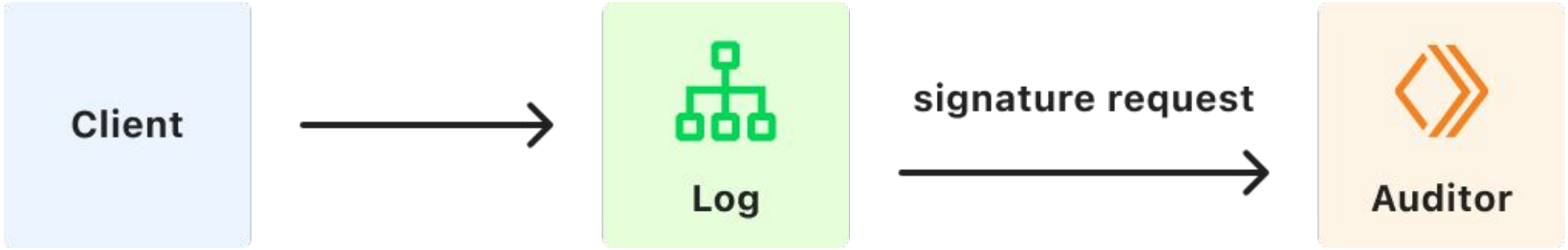
Key Transparency components - 0



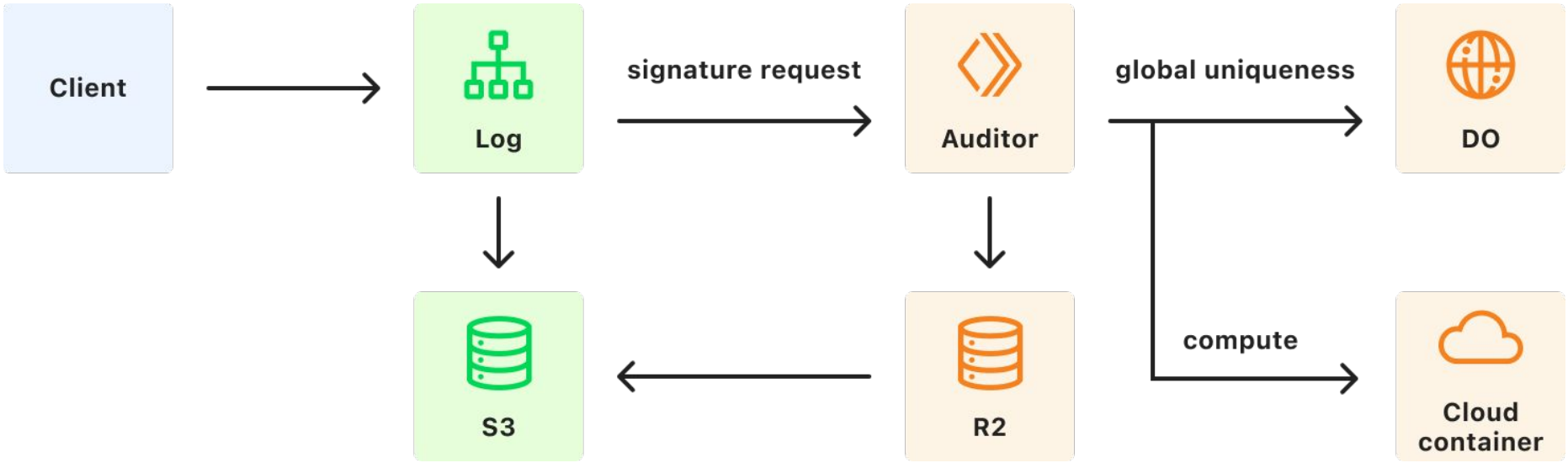
Key Transparency components - 1



Key Transparency components - 2



Key Transparency components - 3



Section

Demo

Thank you

Blog post:
https://blog.cloudflare.com/key-transparency/

Documentation:
https://developers.cloudflare.com/key-transparency/

Dashboard:
https://dash.key-transparency.cloudflare.com/

GitHub:
https://github.com/cloudflare/plexi/