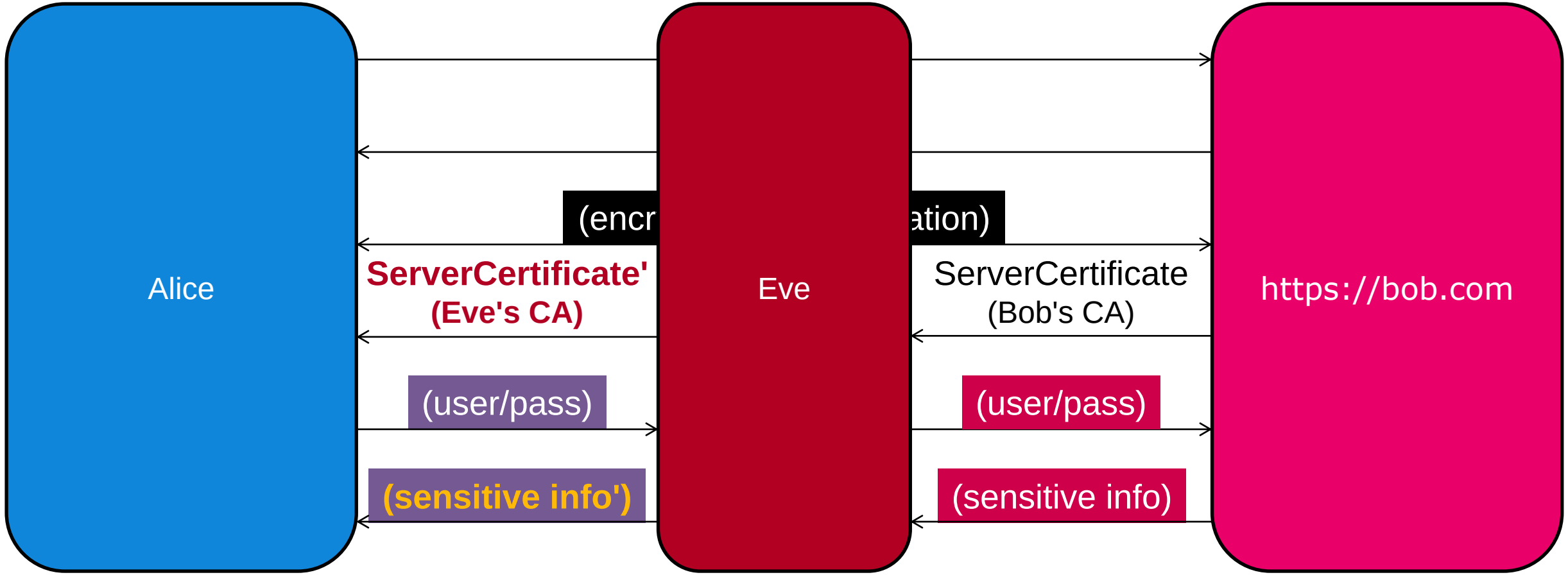
CAPS: Smoothly Transitioning to a More Resilient Web PKI

Stephanos Matsumoto*, Jay Bosamiya^, Yucheng Dai^, Paul van Oorschot§, Bryan Parno^

*Olin College of Engineering, ^Carnegie Mellon University, §Carleton University

Introduction: MITM Attacks in the Web PKI



Introduction: Deployability vs. MITM Prevention

- Certificate Transparency (RFC 6962)
  - Easy to detect misissued certificates
  - Wid
  - PK
  - *Doe*
  - *No w*

- ARPKI (Basin et al., CCS 2014)
  - Prevents MITM despite *n* malicious CAs
  - tees
  - *issuance*
  - *ssibility*
  - *ntication*

How can we smoothly deploy improvements to the Web PKI to prevent MITM attacks?

- Prevent MITM attacks by establishing "authoritative keys"
- Keep domains accessible even if misconfigured/attacked
- Resist downgrade attacks that force use of the current PKI

Certificates with Automated Policies and Signaling

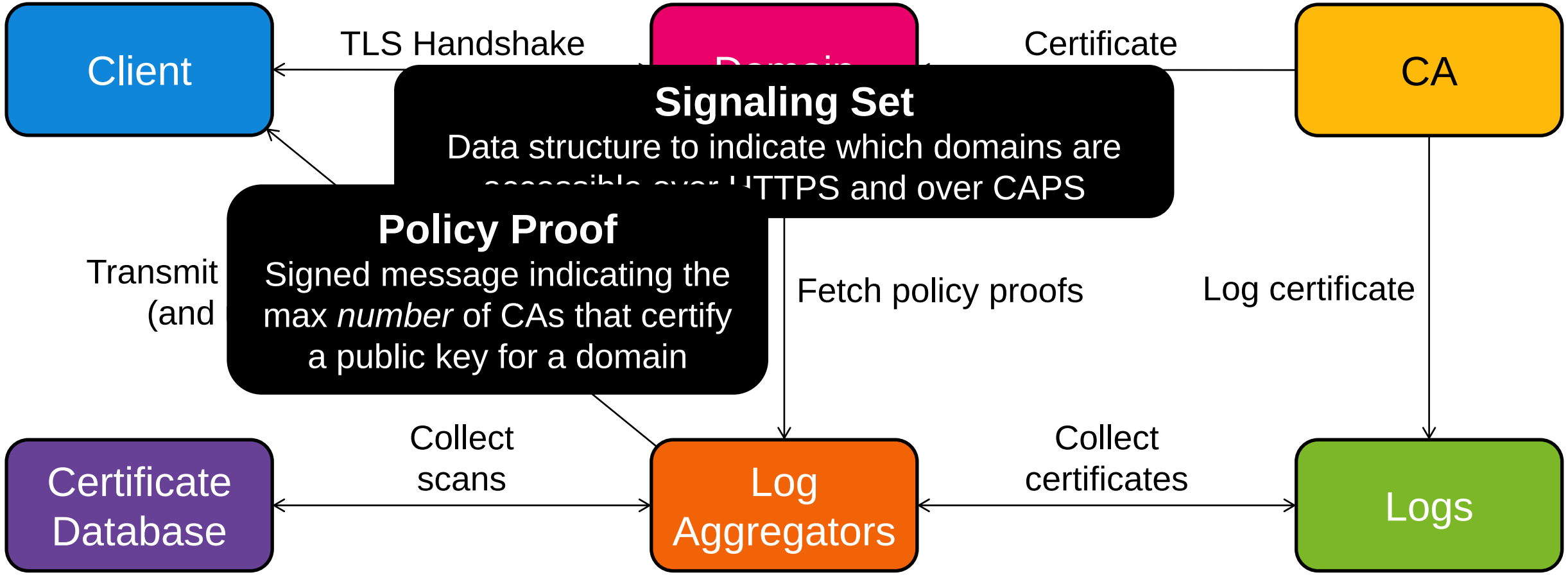
Use **global, public logging as a communication channel** for domains and CAs

Signal deployment of **both HTTPS and CAPS** using a global view of the Web PKI

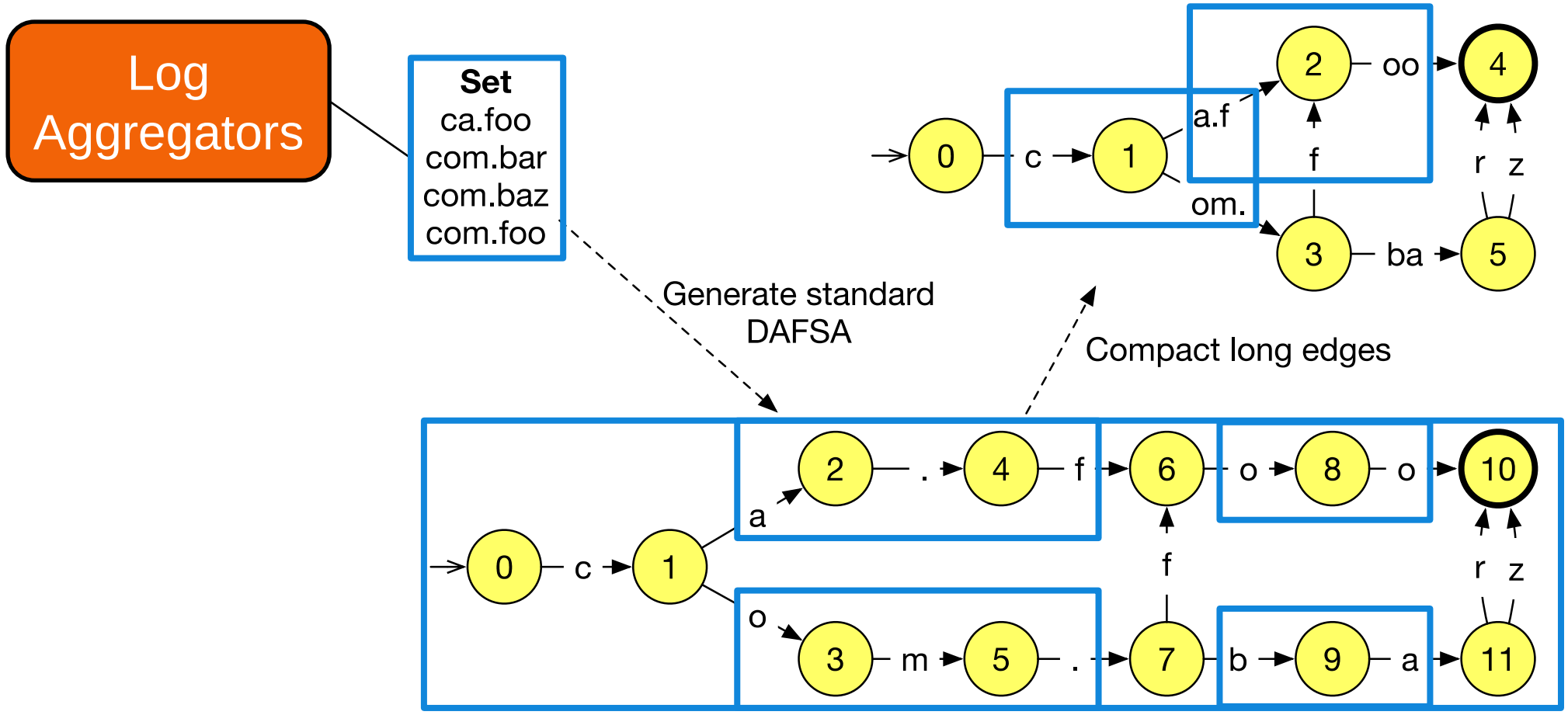
Leverage the **existing PKI to establish authoritative public keys** for each domain

Bootstrap deployment of Web PKI improvements using authoritative public keys

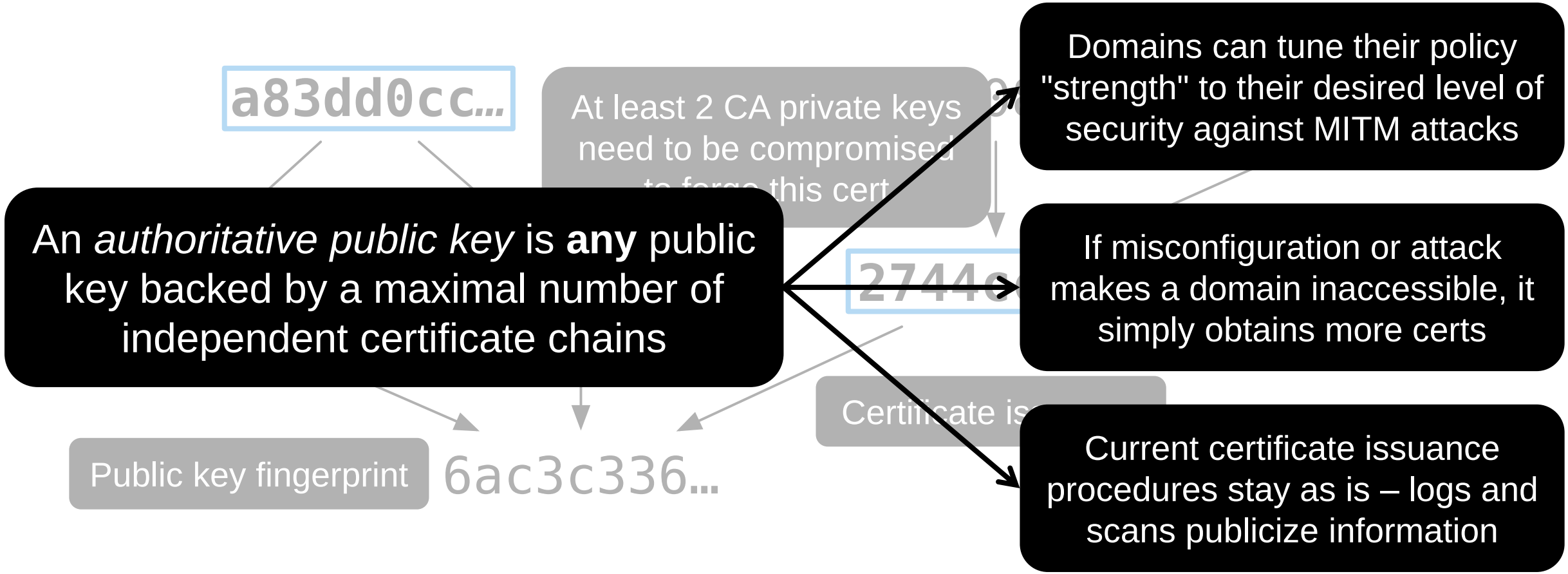
CAPS: Architecture and Overview



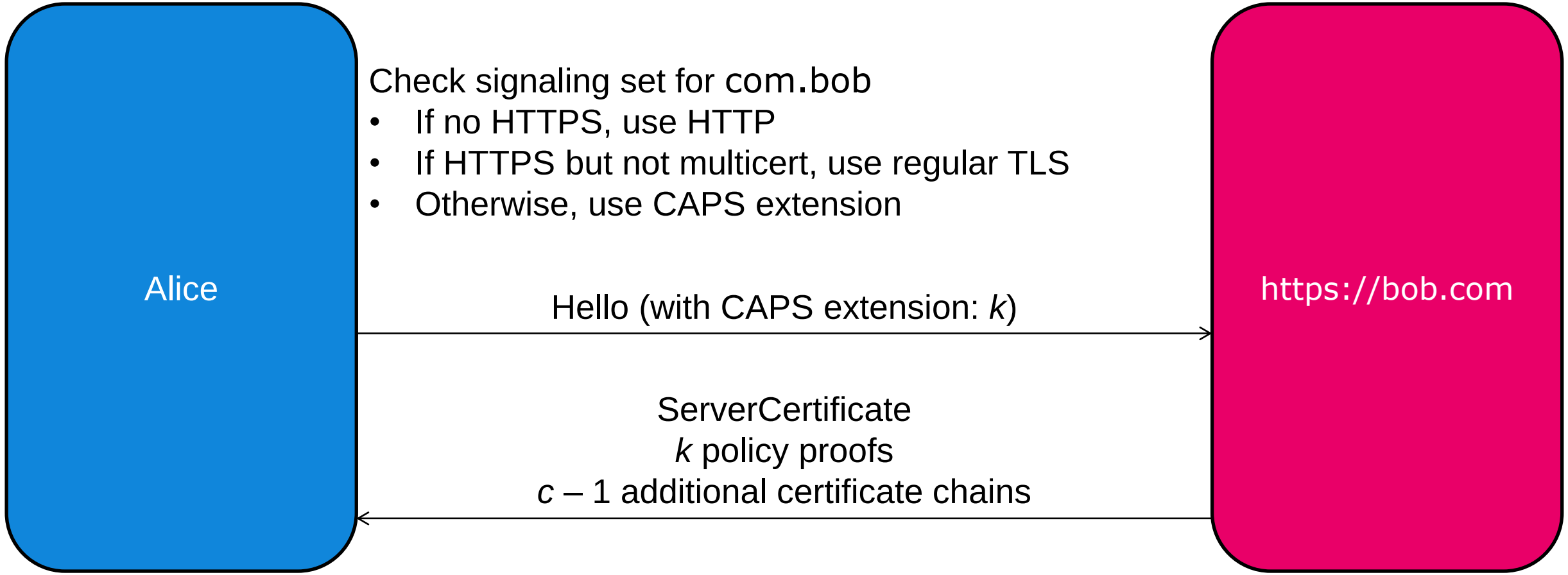
CAPS: Constructing the Signaling Set



CAPS: Building the Policy Database



CAPS: Connection Establishment

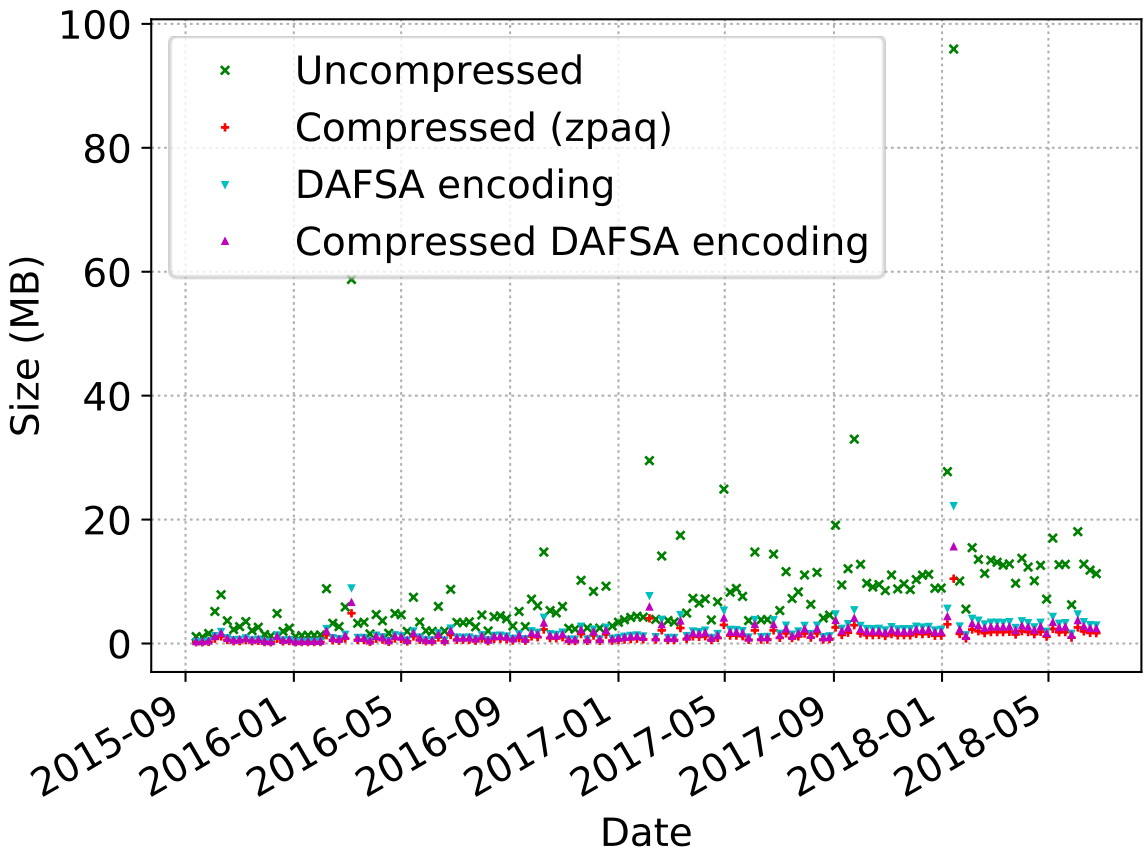


Evaluation: Signaling Set Construction

64,050,329 DNS names as of July 2018

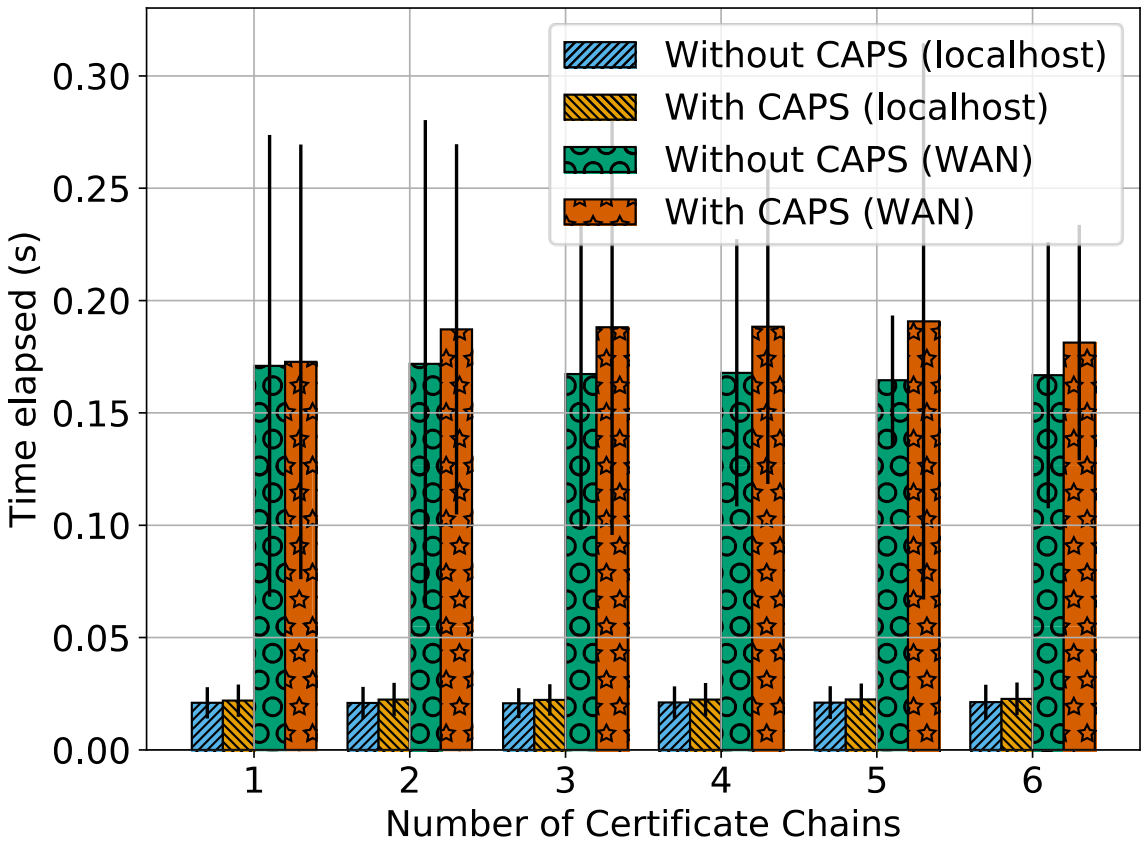
Representation	Size (MB)
Plaintext	1,509
zpaq (best-case compression)	104
DAFSA	**190**
DAFSA + zpaq	**148**

zpaq has better on-disk size, but DAFSA can be used as-is in memory when querying



Evaluation: Connection Establishment Overhead

- nginx/curl: isolate effects of CAPS signaling set/extension
- localhost: loopback interface (lower bound on added latency)
- WAN: single client and VPS (realistic estimate of added latency)
- ~5% increase in latency on average
  - localhost: ~1.2ms
  - WAN: ~11ms



Conclusions

CAPS uses global view of Web PKI to **signal deployment and prevent downgrade attacks**

Flexible CAPS policies prevent MITM attacks **while avoiding pitfalls of misconfiguration**

Thank you!

smatsumoto@olin.edu

https://github.com/syclops/caps

CAPS imposes only **modest overhead on storage, memory, and handshake latency**

CAPS provides for a **secure, smooth transition to a more resilient Web PKI**