BEFORE I BEGIN…

- In 3-weeks for my FI seminar,

  Road to decentralized Public Key Infrastructure (D-PKI)

- Problems with Centralized PKI (C-PKI)
  - Single point of failure, large attack surface, different registration/renewal methods per service providers, revocation/equivocation
  - Managing multiple PKIs (web, cloud, privately maintained, etc.) are a headache
  - Can we detect certificate misissuance? → CT (Certificate Transparency) logs
    - ✓ *F-PKI: Enabling Innovation and Trust Flexibility in the HTTPS Public Key Infrastructure*
  - Can we trust CAs? → CCADB (Common CA Database)
    - ✓ *What's in a Name? Exploring CA Certificate Control*
- Most D-PKI involves the usage of blockchain/DLT (B-PKI)
- In a nutshell… **Enhancing PKI through Ethereum smart contracts**

MMLAB MAIN SEMINAR

IKP: TURNING A PKI AROUND WITH DECENTRALIZED AUTOMATED INCENTIVES

STEPHANOS MATSUMOTO[1,2] AND RAPHAEL M. REISCHUK[2]
1 CARNEGIE MELLON UNIVERSITY 2 ETH ZURICH

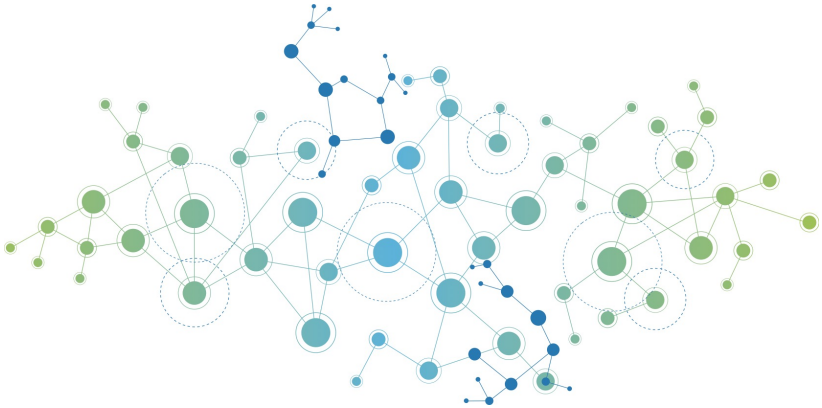
IEEE S&P 2017

Hyunsoo Kim (hskim@mmlab.snu.ac.kr)

2022. 05. 18

서 울 대 학 교
SEOUL NATIONAL UNIVERSITY

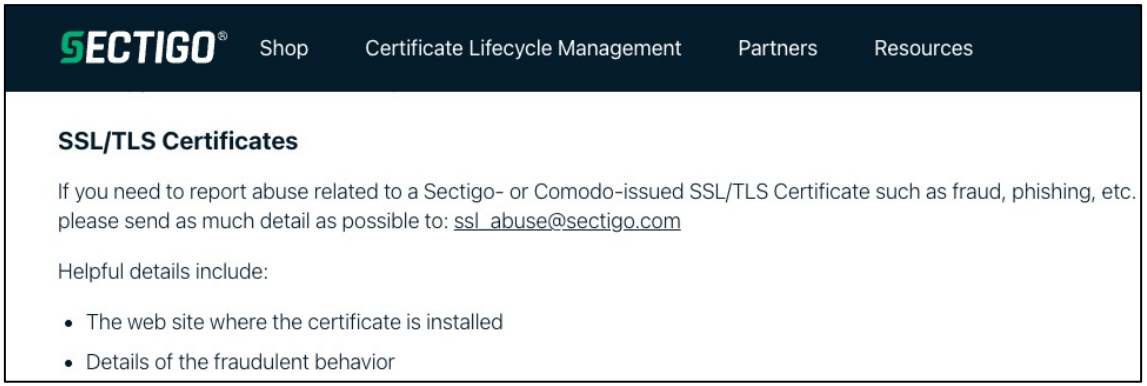
mmLab
Network Convergence & Security Lab



Contents

Problems in the WebPKI

- Reporting misissued certificates is time- and labor-intensive



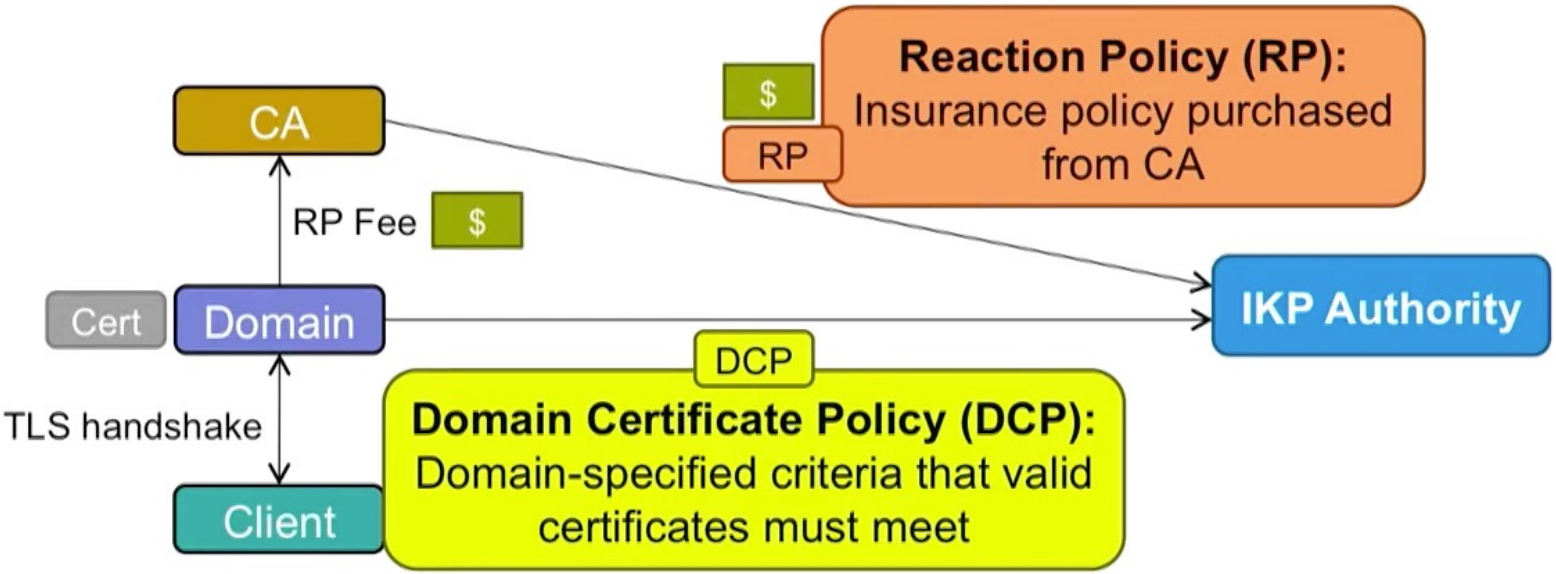
- How can we automatically handle and incentivize reports of misissued certificates?
- Not just certificates but also CAs
  - E.g. Symantec misissues 2,645 certificates for both existing(incl. Google) and unregistered domain names
  - CAs do not have the incentives and deterrents necessary for correct behavior
- How can we incentivize correct behavior and deter misbehavior in the TLS PKI?

INSTANT KARMA PKI (IKP)

- Auditability: all information required to detect misbehavior is public
- Automation: react to CA misbehavior without additional action
- Incentivization: rewards to good CAs and for exposing misbehavior
- Deterrence: guaranteed punishment for misbehaving parties

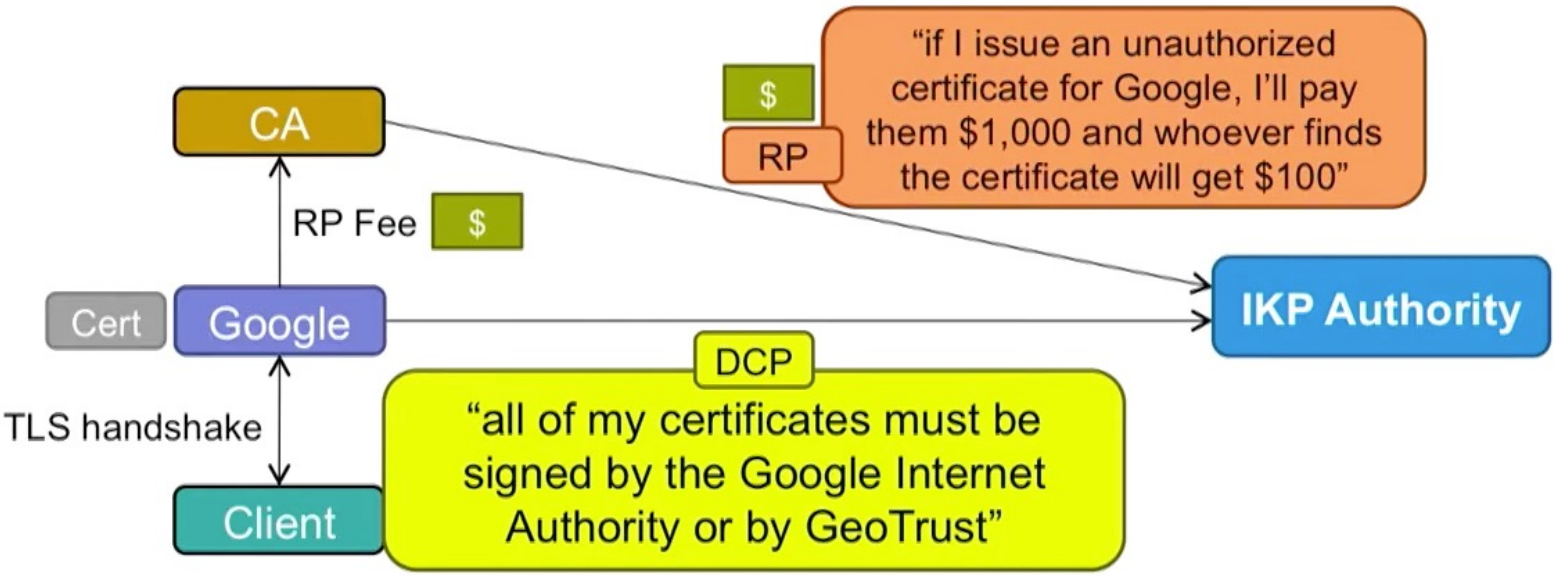
IKP Overview

- Architecture



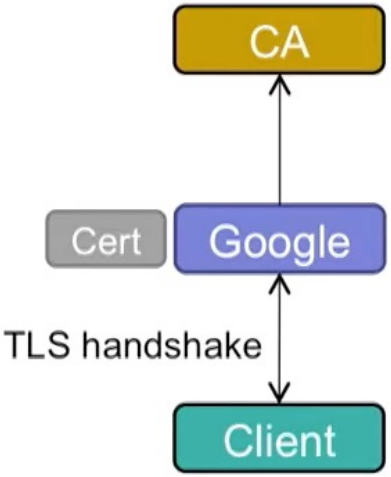
IKP Overview

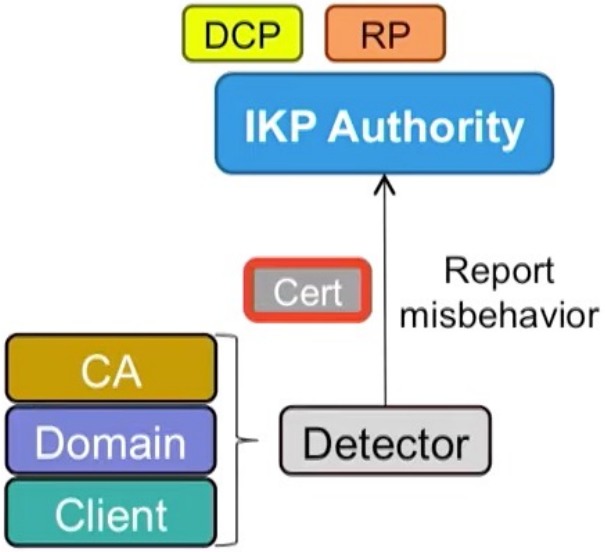
- Example



IKP Overview

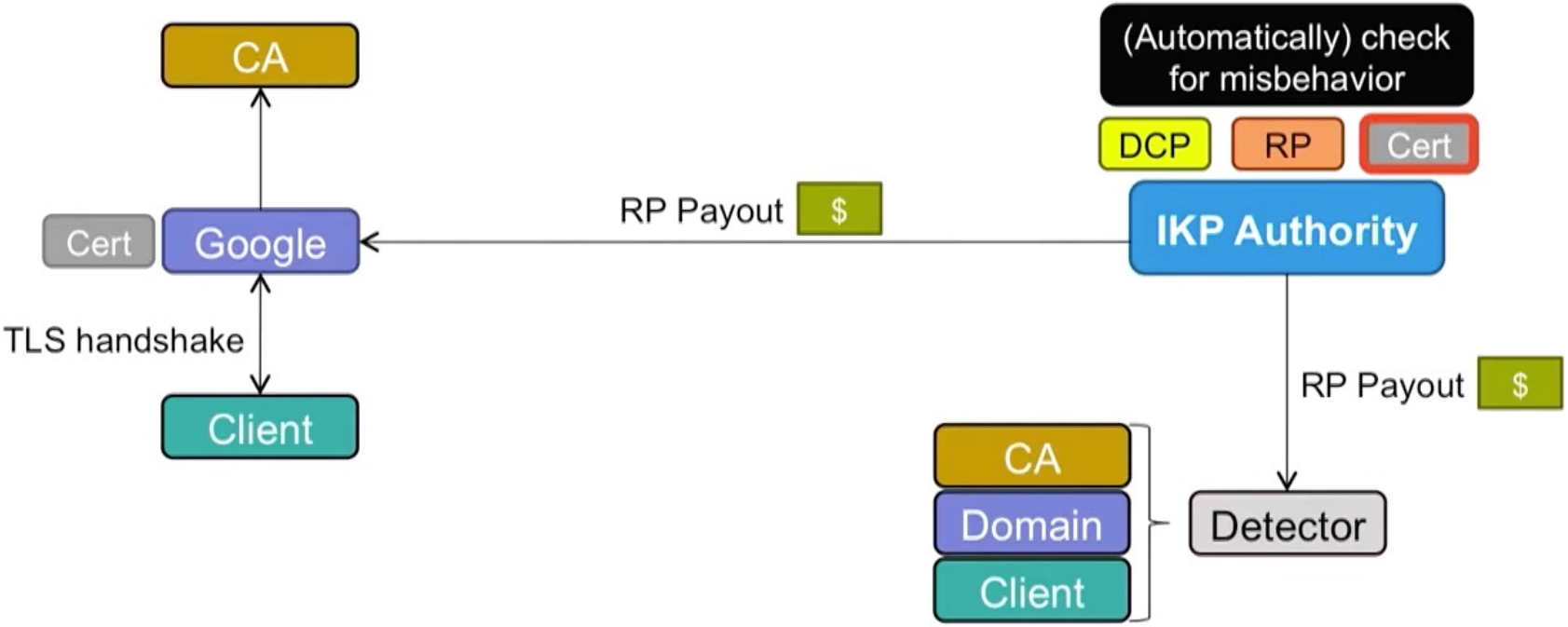
- Example RP payout





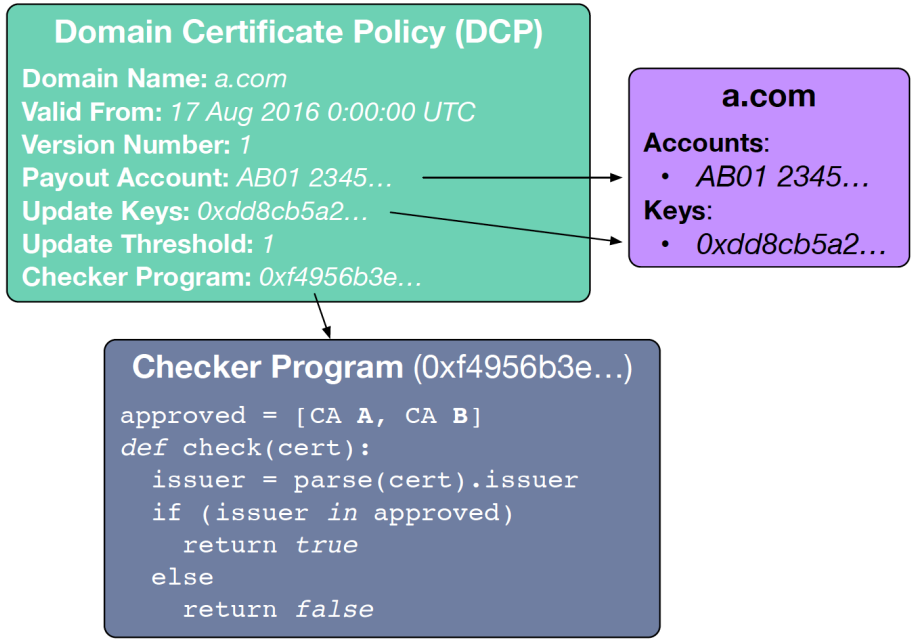
IKP Overview

- Example RP payout



Domain Certificate Policies (DCPs)

- Domains publicize certificate criteria
- Financial account information enables automatic payouts
- Checker program (smart contract) allows expressive range of policies
- Protected from tampering by threshold signature scheme

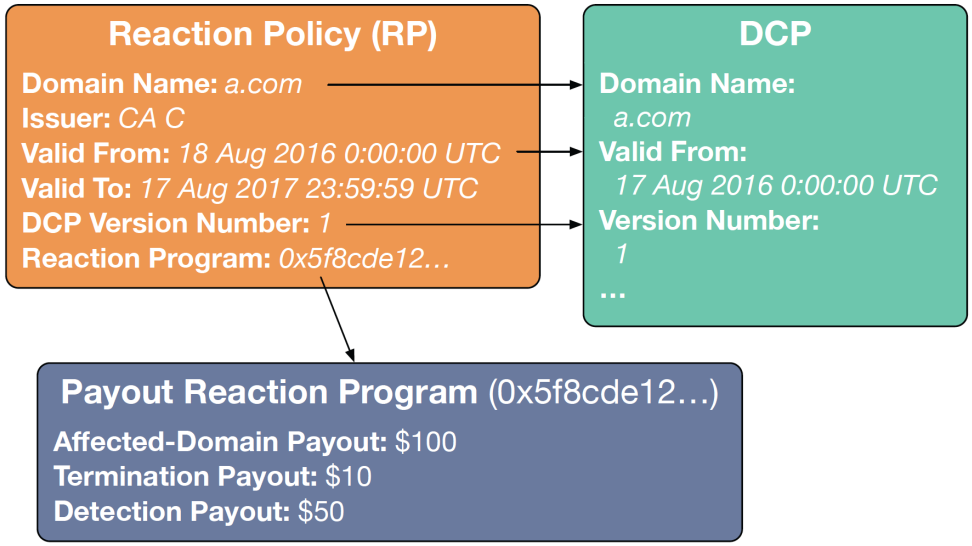


BOOTSRAPING DCPS

- How can we ensure that a domain firstever submitting a DCP is legit?
- Allowing any DCPs to be registered could cause problems
- Bootstrap proofs
  - Protect integrity of initial DCP registration
  - Domains send certificate chain(s) anchored in a known root CA key
  - Registrations can be overriden with more independent chains
  - Example)
    1. Alice claims mmlab.snu.ac.kr is her domain, provides a verifiable certificate chain, which is actually corrupted
    2. $\text{MMLAB\_DCP}_{\text{Alice}}$ is successfully registered
    3. Bob claims mmlab.snu.ac.kr is his domain, provide two verifiable certificate chain
    4. IKP authority overrides $\text{MMLAB\_DCP}_{\text{Alice}}$ with $\text{MMLAB\_DCP}_{\text{Bob}}$

REACTION POLICIES (RPS)

- Purchased from CAs, negotiated between the domain and the CA
- Independent of certificates issuance
- For one instance of misbehavior
- Payouts program (smart contract)
  - {Affected-Domain, Termination} payout: CA → Domain
    - ✓ Domains who fell victims of unauthorized certificates
  - Detectors payout: CA → Detector
    - ✓ Paid to whomever reports an unauthorized certificate issued by IKP CA

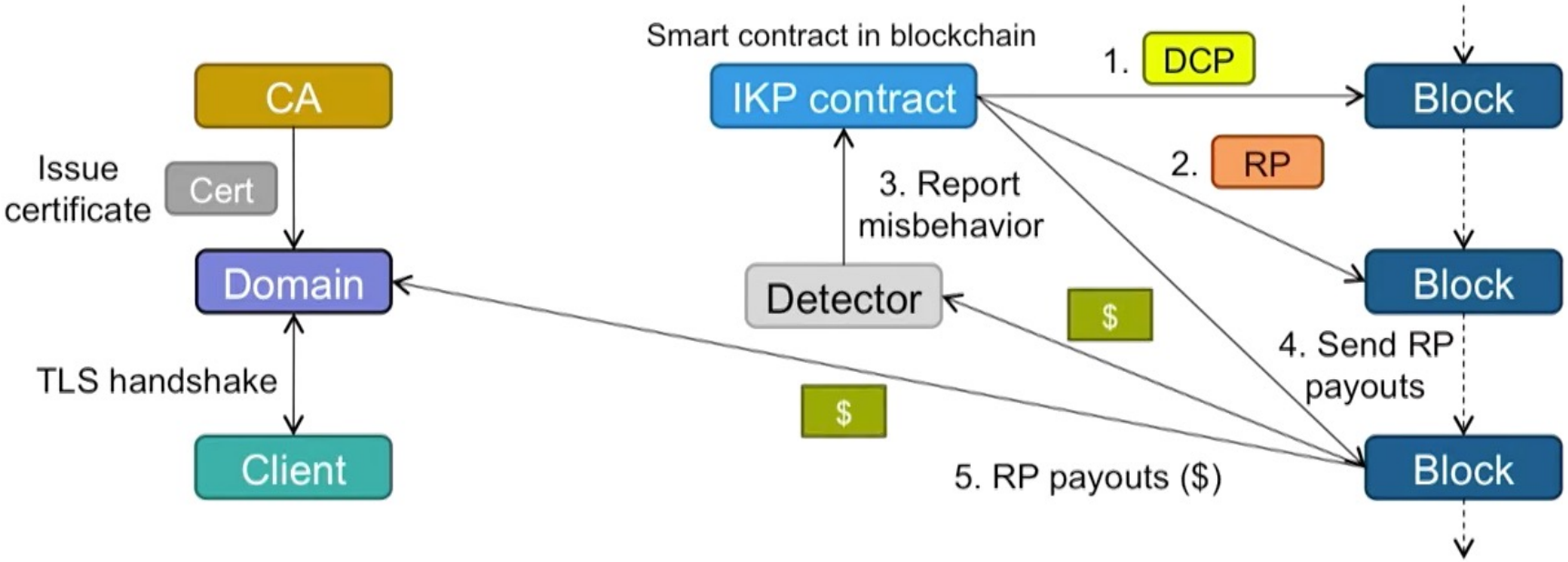


INCENTIVES IN IKP

- Carefully designed to provide financial gurantees
- CAs
  - Paid for correctly issuing a certificate in IKP
    - ✓ Gain a business edge over free CAs like [Let's Encrypt]
  - Cannot profit by collustion with domains/detectors
- Detectors
  - Profit from reporting a misissued certificate
  - Fined for spuriously reporting certificates

IKP IN ETHEREUM

- Design overview



IMPLEMENTATION

- Prototype in Solidity (*Github link is dead*)
  - Only handled certificates with SHA-256 hash and RSA signatures
  - Relies on RSA verification as Ethereum Virtual Machine (EVM) primitive
- IKP operations are cheap
  - One-time IKP deployment cost: $4.55 @ 2017
  - Operational costs were a small fraction of certificate costs
  - Even considering the 10x price increase of ETH → $45 for IKP deployment

Operation	Approx. Cost (USD)
CA registration	$0.2507
CA update	$0.0950
DCP registration	$0.5830
DCP update	$0.4970
RP creation	$0.6223
RP termination	$0.2728
Pre-report misbehavior	$0.1754
Report misbehavior	$0.4094
Send RP payouts	$0.2961

CA	Certificate	Cost
Highest-Risk		
GlobalSign [5]	Wildcard	$849
GlobalSign	DomainSSL	$249
StartCom [9, 71]	Ext. Validation	$199
StartCom	Org. Validation	$119
Entrust [7]	Wildcard	$699
...	...	...
Certum [3]	Commercial SSL	$25
Starfield [8]	Standard SSL	$7
Comodo [4]	EV SSL	$99
IdenTrust [6]	Multi Domain SSL	$299
IdenTrust	Standard SSL	$99

Conclusion and Critique

- Auditability: DCPs and RPs live on the Ethereum blockchain
- Automation: IKP authority implemented as a smart contract
- Incentivization: payouts align incentives with desired behavior
- Deterrence: misbehaving CAs face public, financial penalties

- Critiques
  - Relying on number of verifiable chains in bootstrap proof is questionable, perhaps using CT logs for membership proof is a better approach
  - Weak or no argument regarding the use of Ethereum, is it necessary to use public PoW-based blockchain?
  - Amounts of incentives/payouts are unclear

감사합니다

Thank you~!