Applications for NDN

James Kasten
University of Michigan

Network Authentication

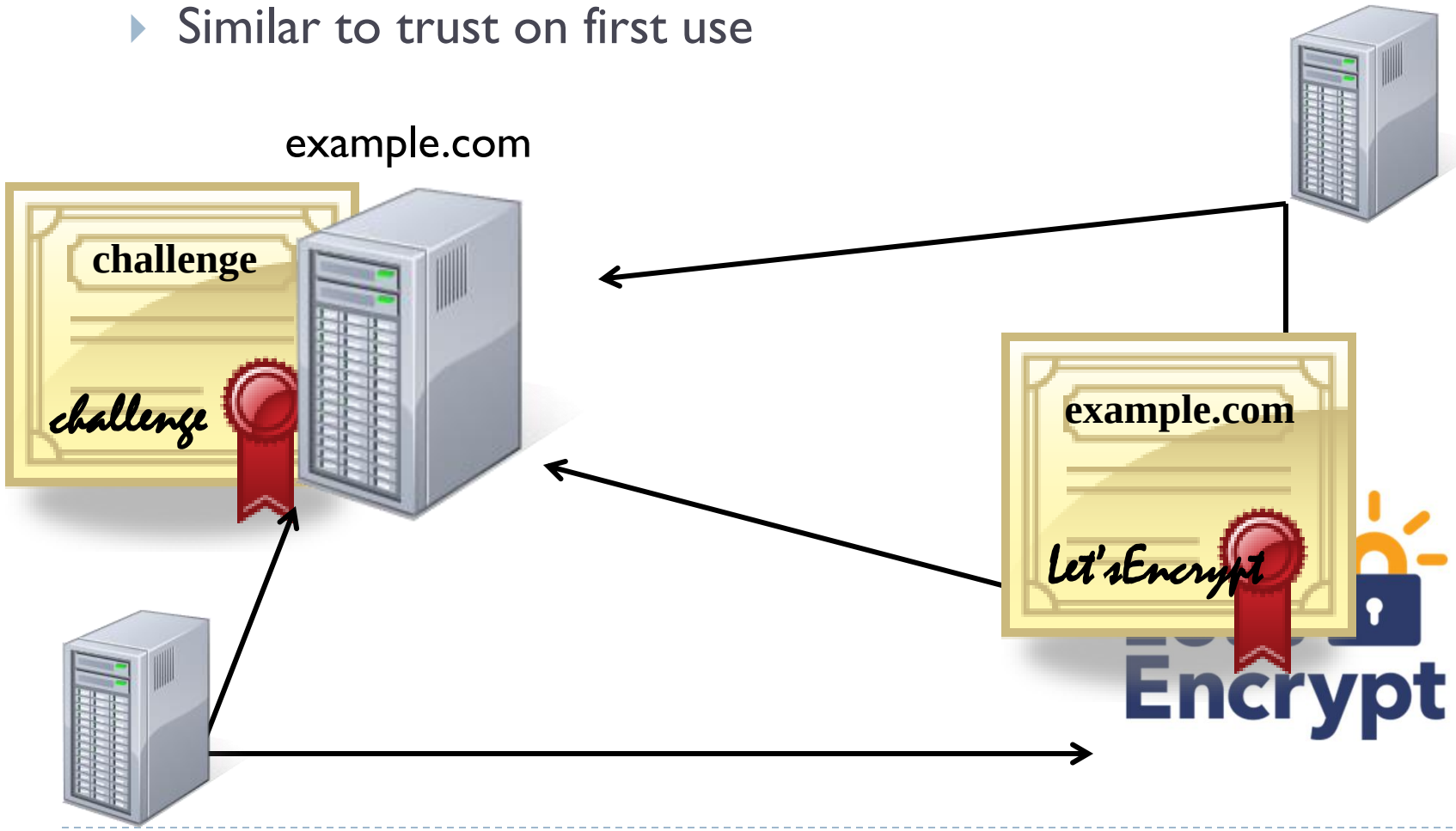
- Public Key Infrastructure
  - Pairing Keys with Identity or Authority
- Major Challenges
  - Management
  - Distribution
  - Revocation
  - Renewal

Let's Encrypt

- New Certificate Authority
  - Open source
  - Simple
  - Automated
    - ACME (new protocol)
      - Verification
      - Issuance
      - Renewal
      - Revocation
- One command to enable TLS
  - sudo letsencrypt

Let's Encrypt Trust Model

- Domain validation (DV)
  - Similar to trust on first use

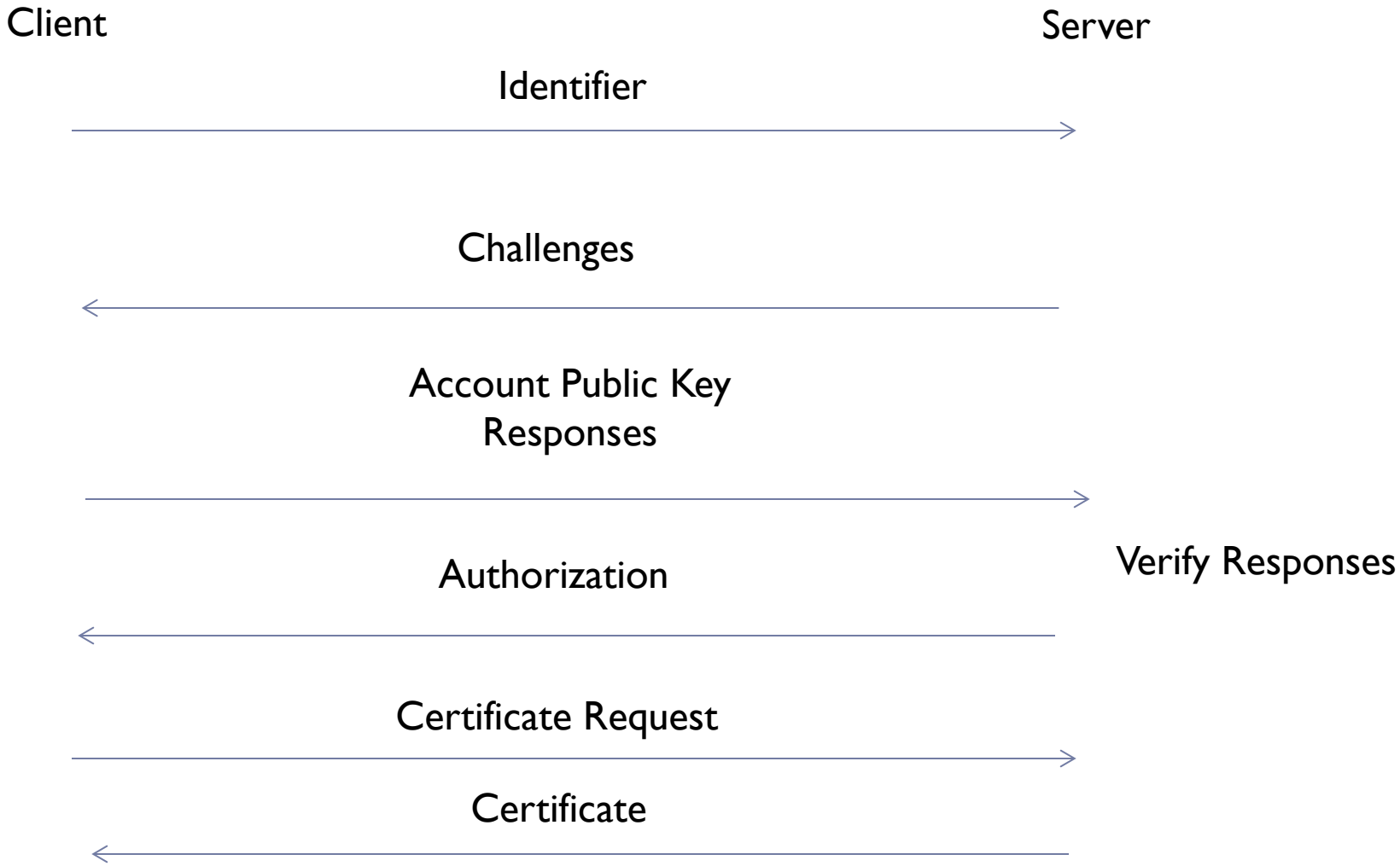


Quick Demo

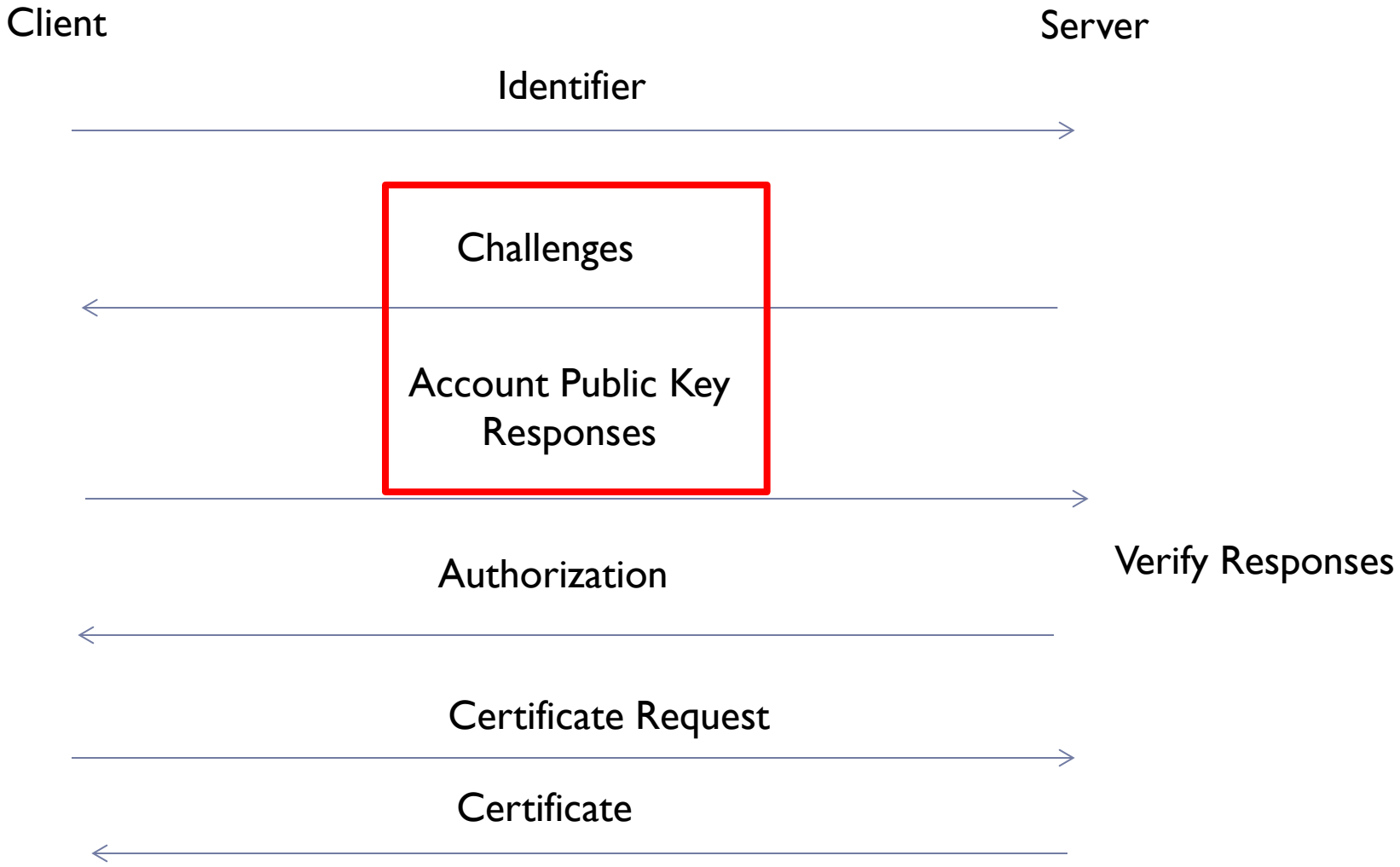
Benefits for NDN

- Authority instantiated out of the box
  - A framework to receive automated authorizations
- Open mHealth
  - Individual service CAs can grant various authorizations
  - Automatically place authorizations in local IdentityManager
- EBAMS
  - Large computing base with few resources
    - ACME is lightweight
    - Local CAs/controllers can propagate trust downwards automatically

High-level ACME Overview



High-level ACME Overview



Potential NDN Challenge Types

- Prove ownership
  - resource being verified
    - Can be flexible to the organization/application
      - Organization or university
        - Demonstrate control of associated email address
      - Localized CAs - EBAMS
        - Simple publishing/receiving content on a particular interface at a particular time
  - previous account or "authorized key"
    - Publish content under known existing key
    - Provide proof of ownership of a trusted account or authorization
    - Recovery Contact (email address)
    - Bearer Token

Integrating ACME into NDN

- Define a suitable set of challenges for NDN
- Define trust models/verification requirements for authorization in applications

- Implementation
  - Code in progress
    - Battle-tested CA source code
    - Extensible client written in Python
  - Necessary Changes
    - Redefine CSR/Signing procedure (different format)
    - Redefine networking code
    - Define NDN specific challenges