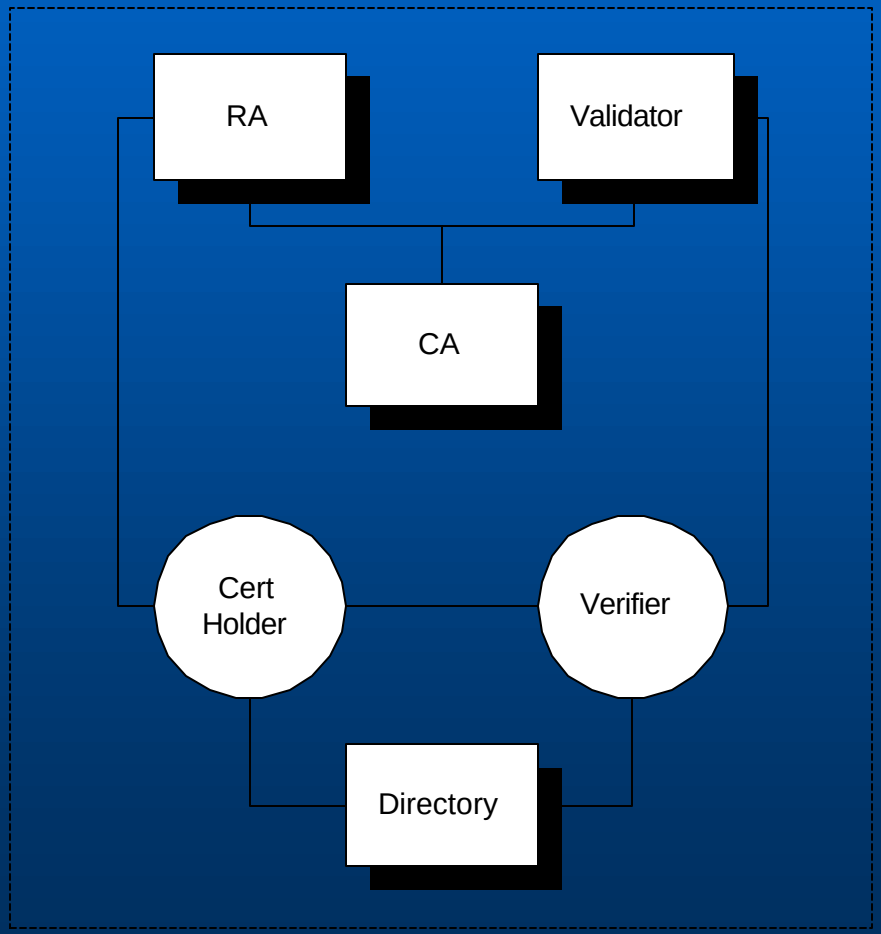
PKI

Managing Trust Extension

Mark Chen
CTO, Securify

Components of a PKI

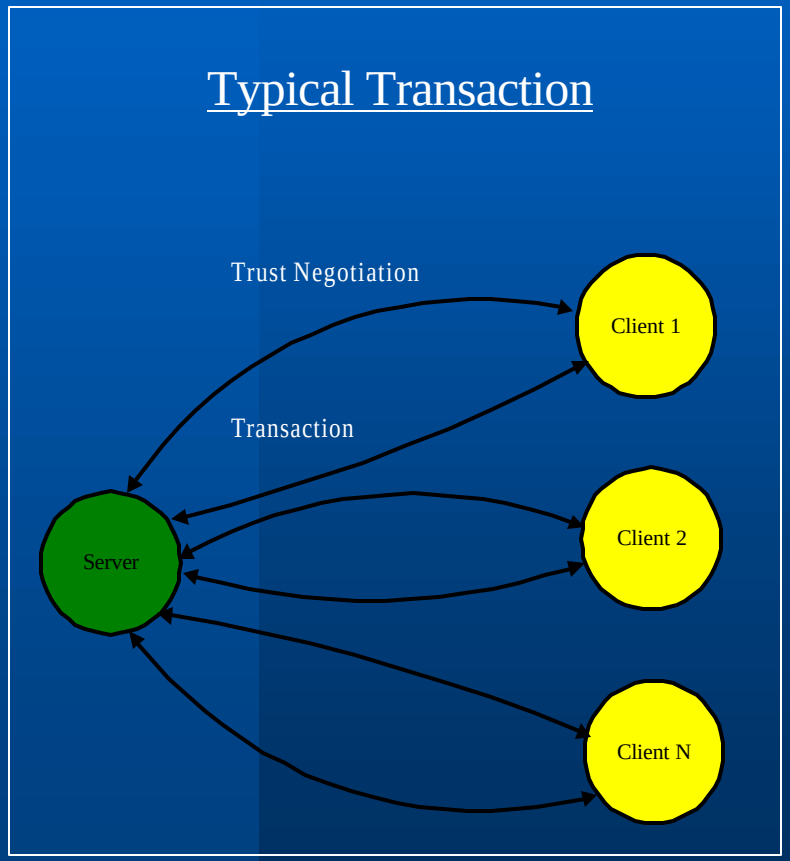


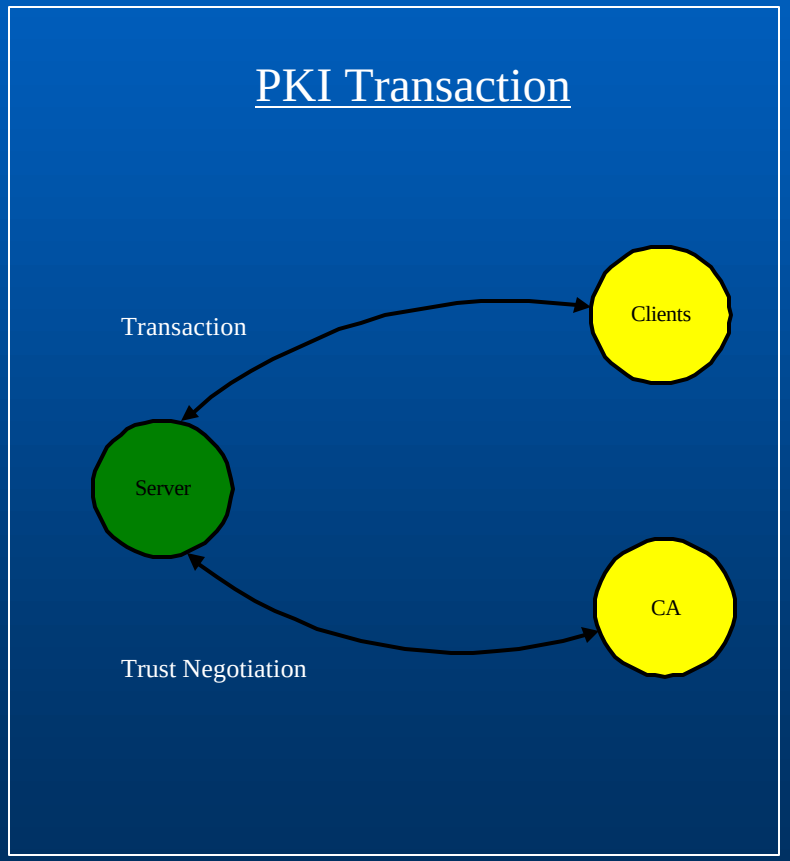
liability

PKI: What It *Appears* to Do

- Remove requirement for out-of-band negotiation
- Provide generalized authentication mechanism

Conventional Transaction vs. PKI Transaction





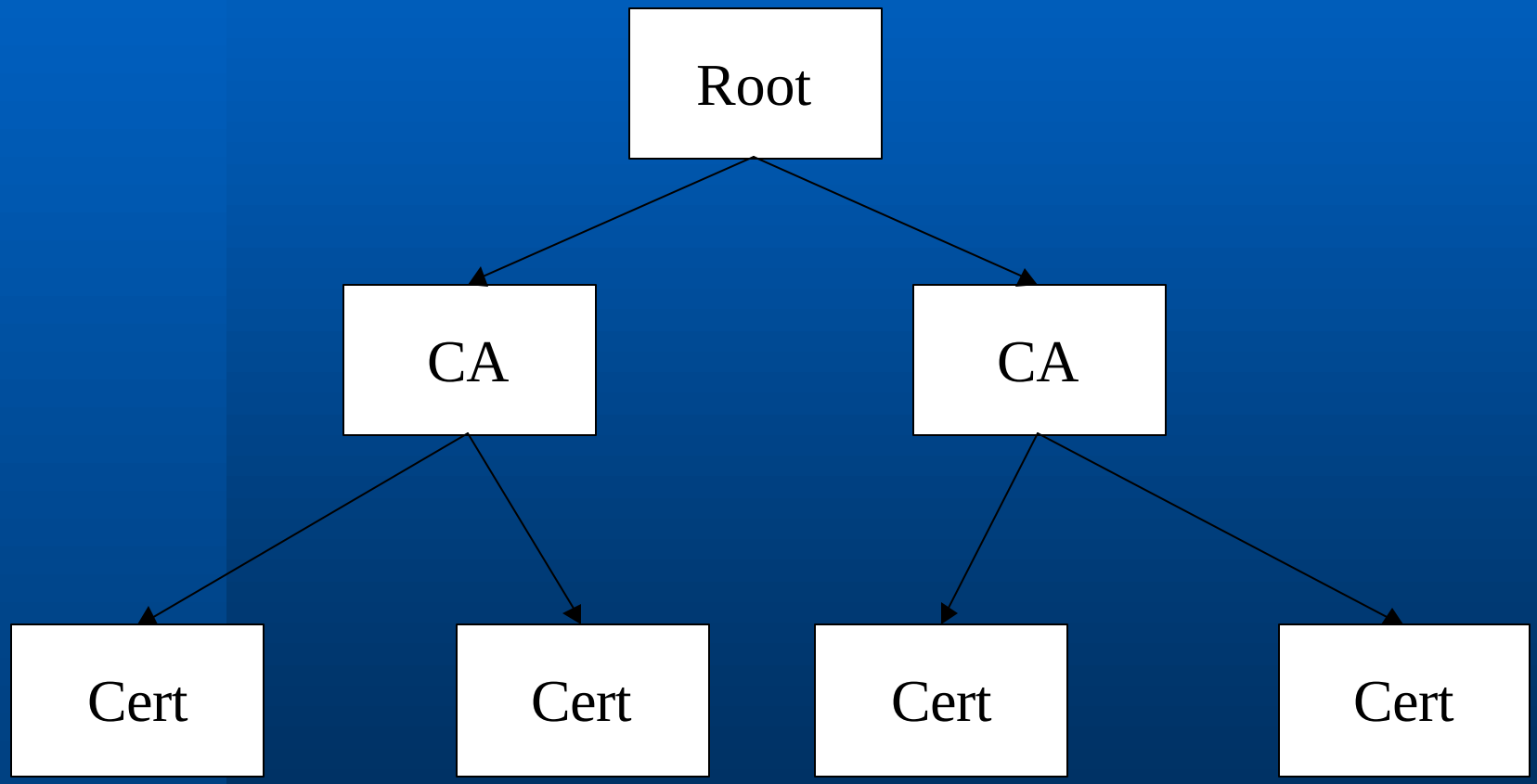
PKI Justifications

- Explicit data-authentication
- Non-repudiation
  - Strong
  - Weak
- Key distribution
- Implementation issues

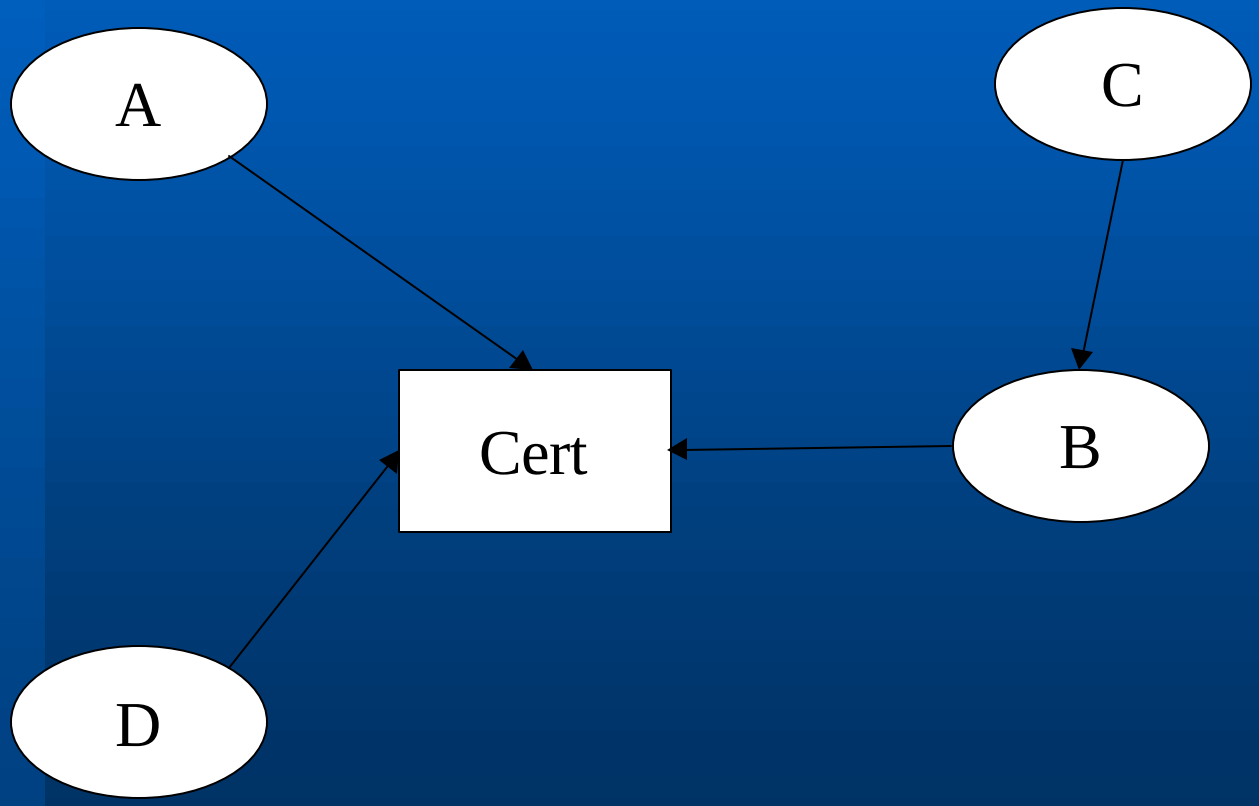
Common Public-Key Algorithms

- Diffie-Hellman
- Elgamal
- DSS
- RSA
- Menezes-Vanstone, etc.

Hierarchical Certification



Relational Certification



Certification Models

- Hierarchical certification (e.g., X.509)
  - Certifiers delegate authority and (should) assume liability
- Relational certification (e.g., PGP)
  - Trust decisions are made by the verifier

Levels of ‘Nymity’

- Anonymity
  - Events are unconnected
- Pseudonymity
  - Events are connected, but the event chain is truncated
- Identity
  - Events are connected to a real person (put another way, the event chain goes all the way back to birth)

Typical Transaction

- Service provider creates key pair and sends public component to CA
- CA creates certificate and sends it to service provider
- Service provider sends certificate to relying party
- Relying party makes trust decision

The CA as Trust Proxy: *Basic Principles*

- Extension of trust requires explicit definition of obligations
- Relying parties must have relief in the case of a failure
- In most cases, the CA does not have explicit bilateral agreements with relying parties

The Certificate Policy: *What It Should Not Do*

- Stipulate extraneous extensions
- Stipulate unparsable extensions
- Contain binding reference to a CPS

The Certificate Policy: *What It Should Do*

- List explicitly all supported applications and protocols
- Be explicit about non-repudiation requirements
- Separate authentication from authorization
- Manage liability
- Hold the CA responsible for its own security

When Is the CA Responsible for Security Failures?

- CA is not responsible
- CA is responsible for compliance with CP
- CA is responsible (period)
- CA is responsible, except for failures resulting from named perils

Three Levels of Validation

- Offline system without validation
  - Possibility of limitless loss cannot be removed
- Online system without validation
  - Individual verifiers can take unilateral action to suspend transactions
- Positive validation
  - Validator is in the transaction stream

How Much Is the CA Responsible for?

- Instance liability cap
- Aggregate liability cap

Summary

- You don’t get something for nothing
- “PKI” is not a universal solution to the authentication problem
- Certification is primarily about liability management, not technology