Building a One-Time-Password Token Infrastructure

Jonathan Hanks & Abe Singer

LIGO Laboratory

LIGO

Distributed

Multi-Institution

International

LIGO

Kerberos

Shibboleth

Grouper

LIGO

Open Data

Time Critical

No Do-Overs

Remote Access

Single/Common sign-on

LIGO

Credential Theft

Separate Credential

Non-Replayable

Not for everything

LIGO

One Time Passwords

What does(n't) OTP solve?

Time Based

Sequence Based

Challenge-Response

One Time Pad

Something you Have

What do(n’t) tokens solve?

Delivery

Rolf

Synchronization

Overhead

Integration

Failures

One token to rule them all

Physical device

Trust No-one

Distributed, Fault tolerant

Open

Cheap

LIGO

Custom Authentication Server

PAM

Yubikey

Kerberos

LIGO

Why?

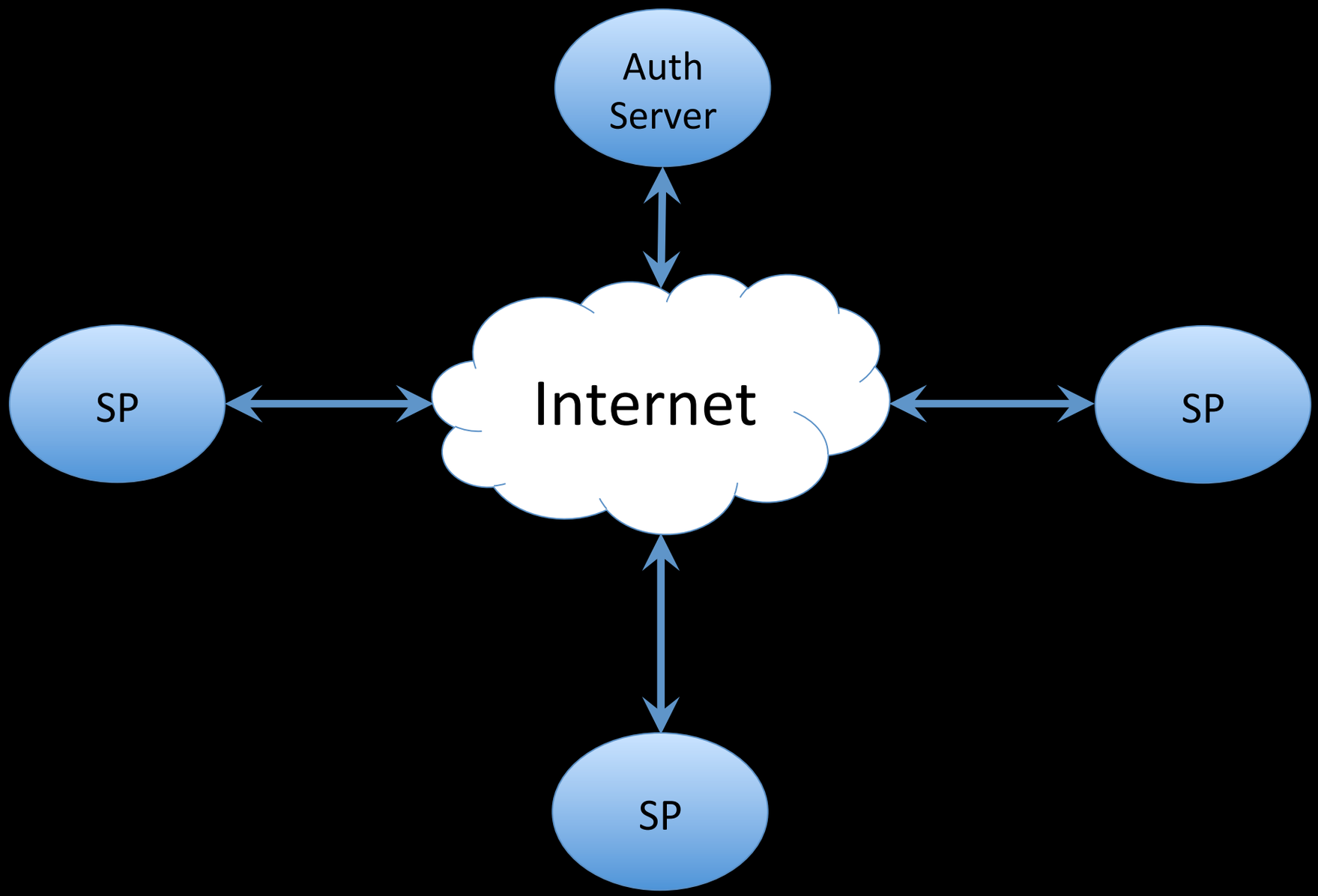
Ownership

Trust

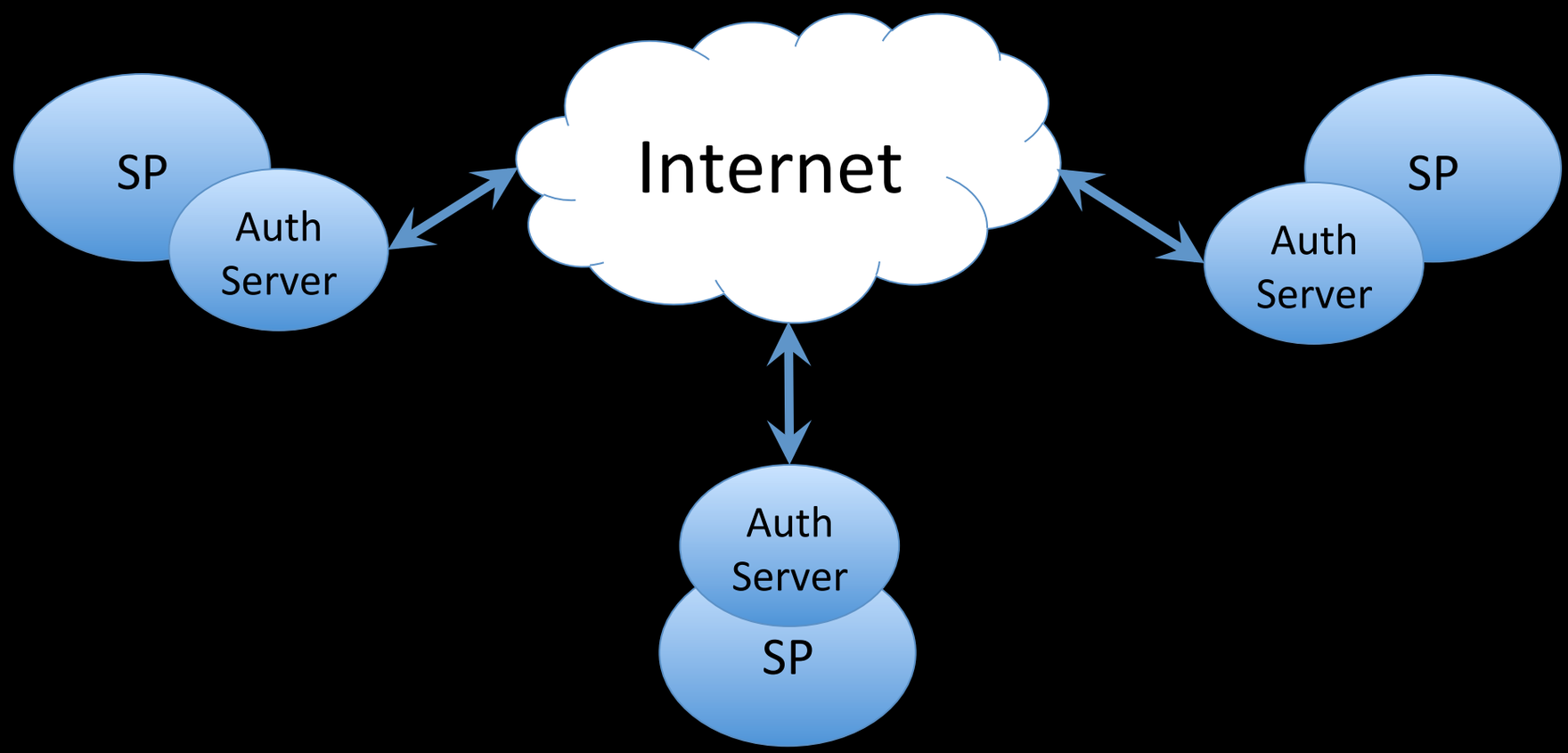
Capabilities

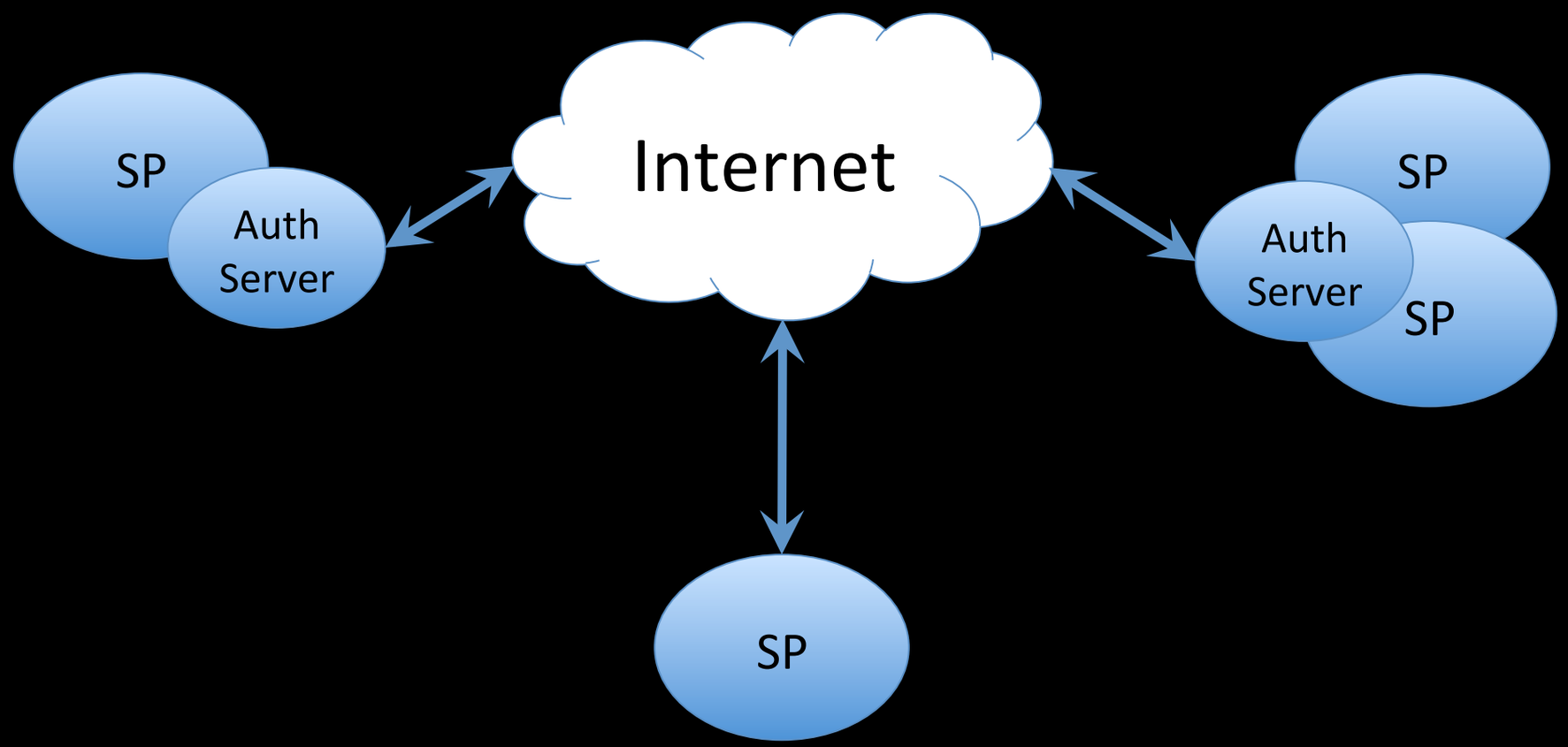
LIGO

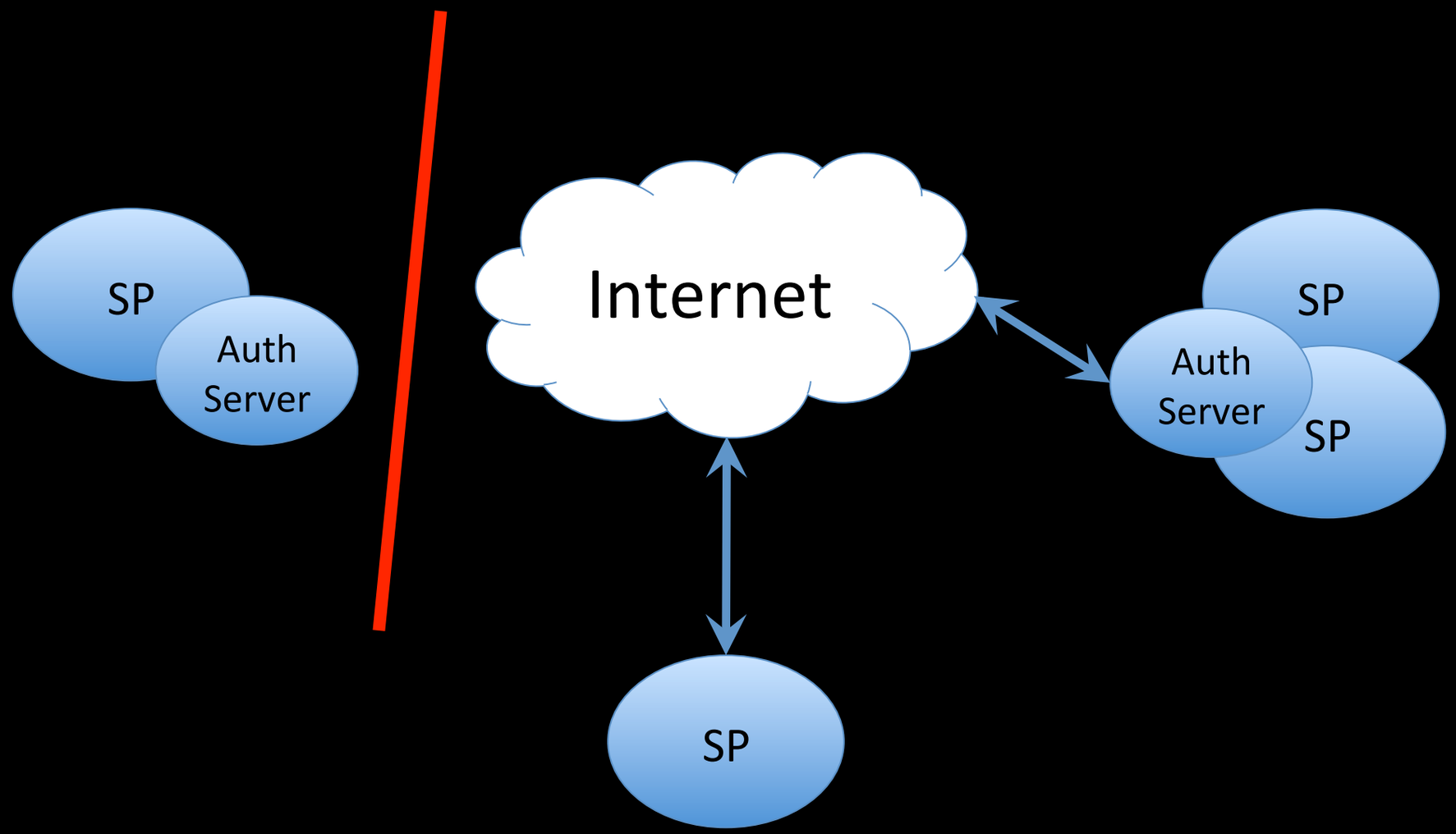
Architectures



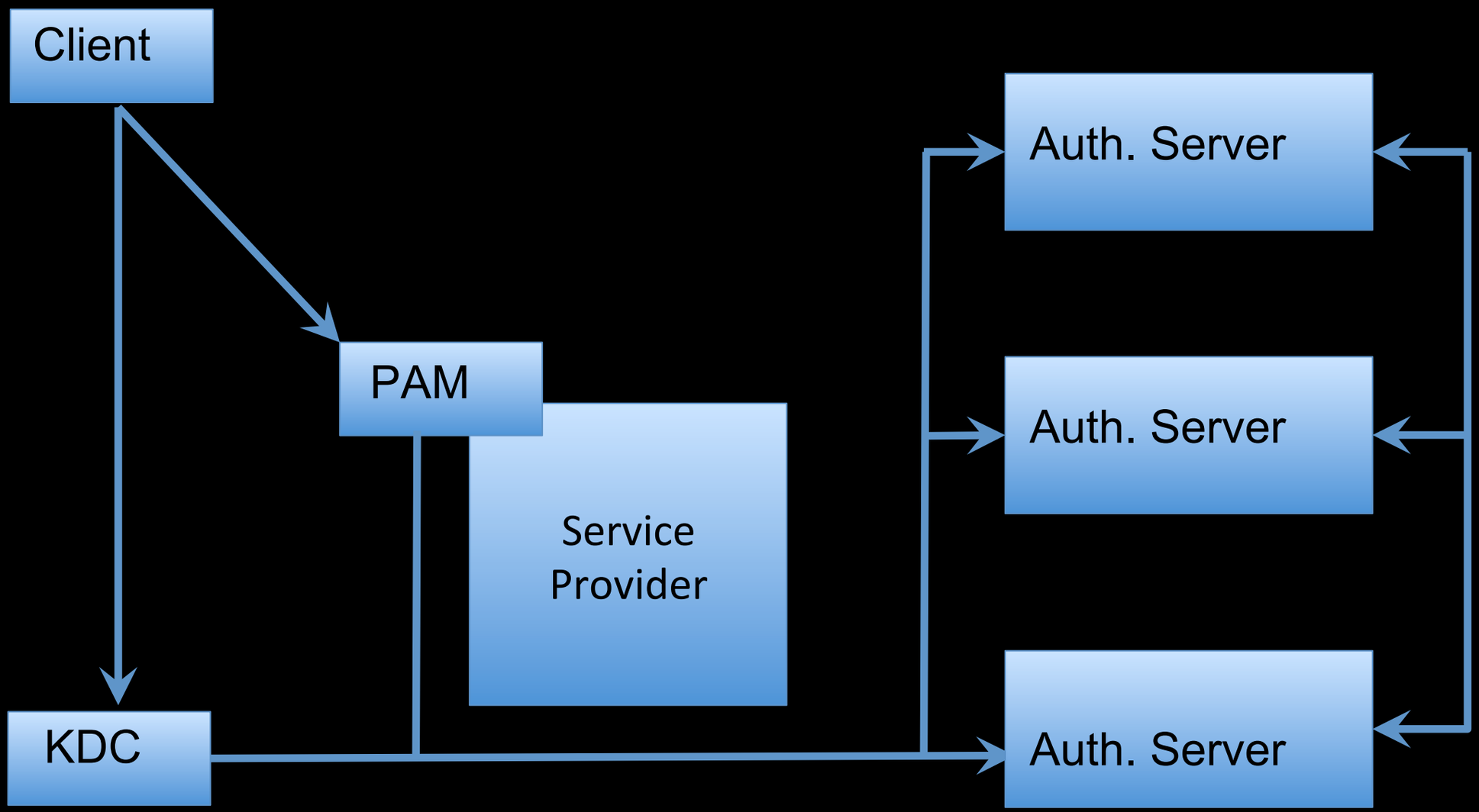
SP = Service Provider


SP
Auth Server
Internet
SP
Auth Server
Auth Server
SP


SP
Auth
Server
Internet
SP
Auth
Server
SP
SP


SP
Auth
Server
Internet
SP
Auth
Server
SP
SP

Architecture



Replication and Mitigating Replay Attacks

Replication takes Time

Replicate Data w/o global locks

Centralized yet Distributed

No Secrets on Endpoints

There can be only one

Modular, Abstracted

LIGO

Provisioning Users

Make it simple

Make it safe

Supporting Users

Any auth scheme is a hinderance

Just replace the token

Experiences / Problems

It Works

Tokens get out of sync

When good tokens go bad

Local Account Issues

LIGO

Kerberos

We like SSO

Cannot afford to support all the client systems

Cannot wait for the OTP extensions to reach end users

LIGO

Hijack encrypted timestamp

All kinits support this

No custom client SW required

Questions?