AfriNIC 14

Shared ccTLD DNSSEC Signing Platform

June 9, 2011

Bill Woodcock

Research Director

Packet Clearing House

ICANN - PCH Common Goals

ICANN Goals:

Accelerate DNSSEC deployment
Maintain the highest standards of security and trust
Squeeze online crime out of developing countries first

PCH Goals:

Support critical Internet infrastructure operators
Increase global network stability and availability
Conduct knowledge-transfer and improve self-sufficiency

Approach

Shared secure signing platform with knowledge transfer

Leverages existing operational expertise within ICANN and PCH

Best-practice implementation, held to the highest standards

No cost, no restrictions: free-as-in-beer and free-as-in-speech

Flexible building-blocks: use the system in part or in its entirety

Clear transition path from shared platform to ccTLD owned-and-operated platform in a single step, or in a gradual process

Benefits

Immediate realization of DNSSEC advantages

Security and auditability on-par with the root zone

Offload several million dollars of components and services

Build experience in a best-practices environment

Take on operational responsibility as you gain confidence

Bidirectional Transition Path

From ccTLD to PCH:
   Under control and guidance of ccTLD
   Clear checklist of transition steps
   KSK and ZSK generated in PCH's HSMs or
   KSK in ccTLD control, ZSKs exported to PCH

From PCH to ccTLD:
   Under stepwise control and guidance of ccTLD
   Clear checklist of transition steps
   KSK and ZSK generated by the ccTLD
   Exchange public key and signature info only
   Transfer of all relevant information

Key Management

Automated signature updates and ZSK rollovers

Automated integrity checking before publication

Real-time monitoring of signing and publication processes

Configurable email alerts on any warning or error

KSK generation and use at offline key ceremonies

Pre-generated keys and signed DNSKEY RRsets
  KSK: 2048 RSA
  ZSK: 1024 RSA NSEC3

Business Continuity & Maintenance

Backup sites on different continents, under diverse control

Well-documented emergency plans
  KSK compromise and loss
  ZSK rollover

Transition plans

DNSSEC Signer Platform

Built on ICANN DNSSEC root-signing design

Conservatively using BIND signing tools

KSKs and ZSKs in FIPS 140-2 Level 4 HSMs

Fully-redundant offline KSK facilities in San Jose and Singapore

Fully-redundant online ZSK facilities in San Jose and Zurich

Bump-in-the-Wire operational model

Clear TLD Transition Plan
   Knowledge-transfer workshops
   Clear checklists for transitioning on and off the platform
   Complete solution including DPS, key management, etc.

Diverse Locations

Americas
San Jose, USA
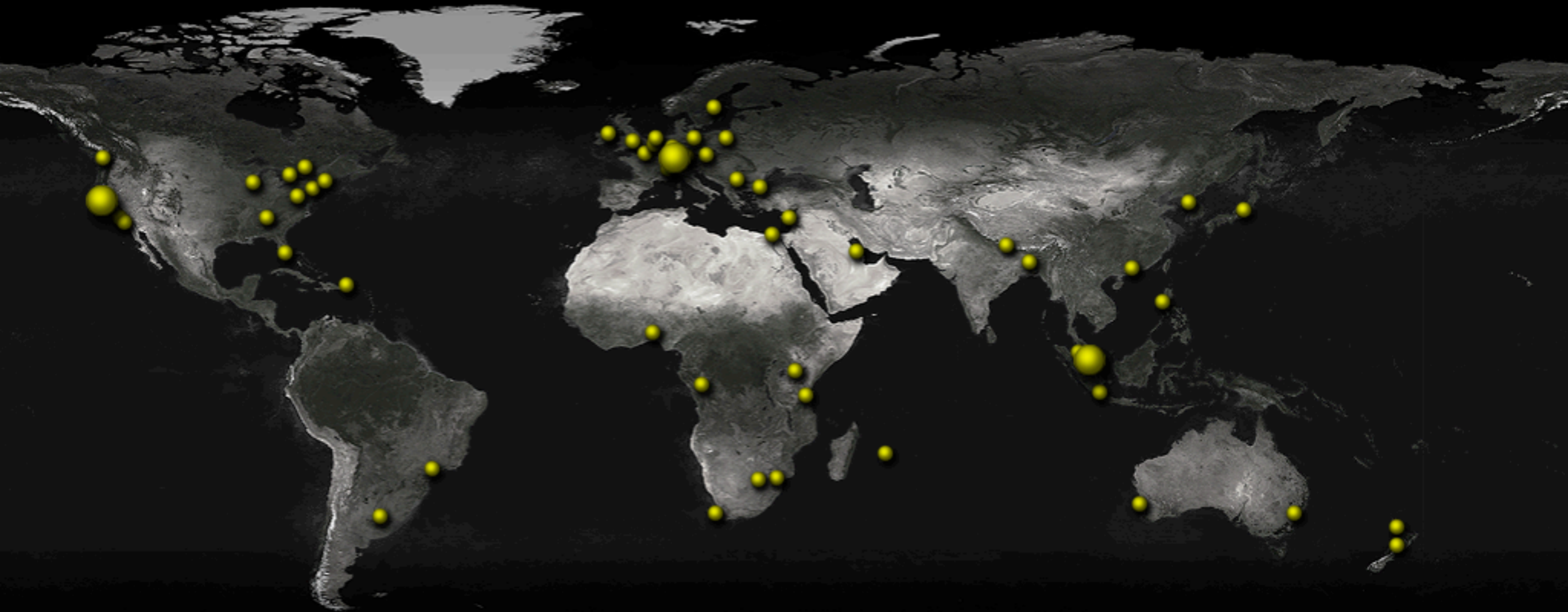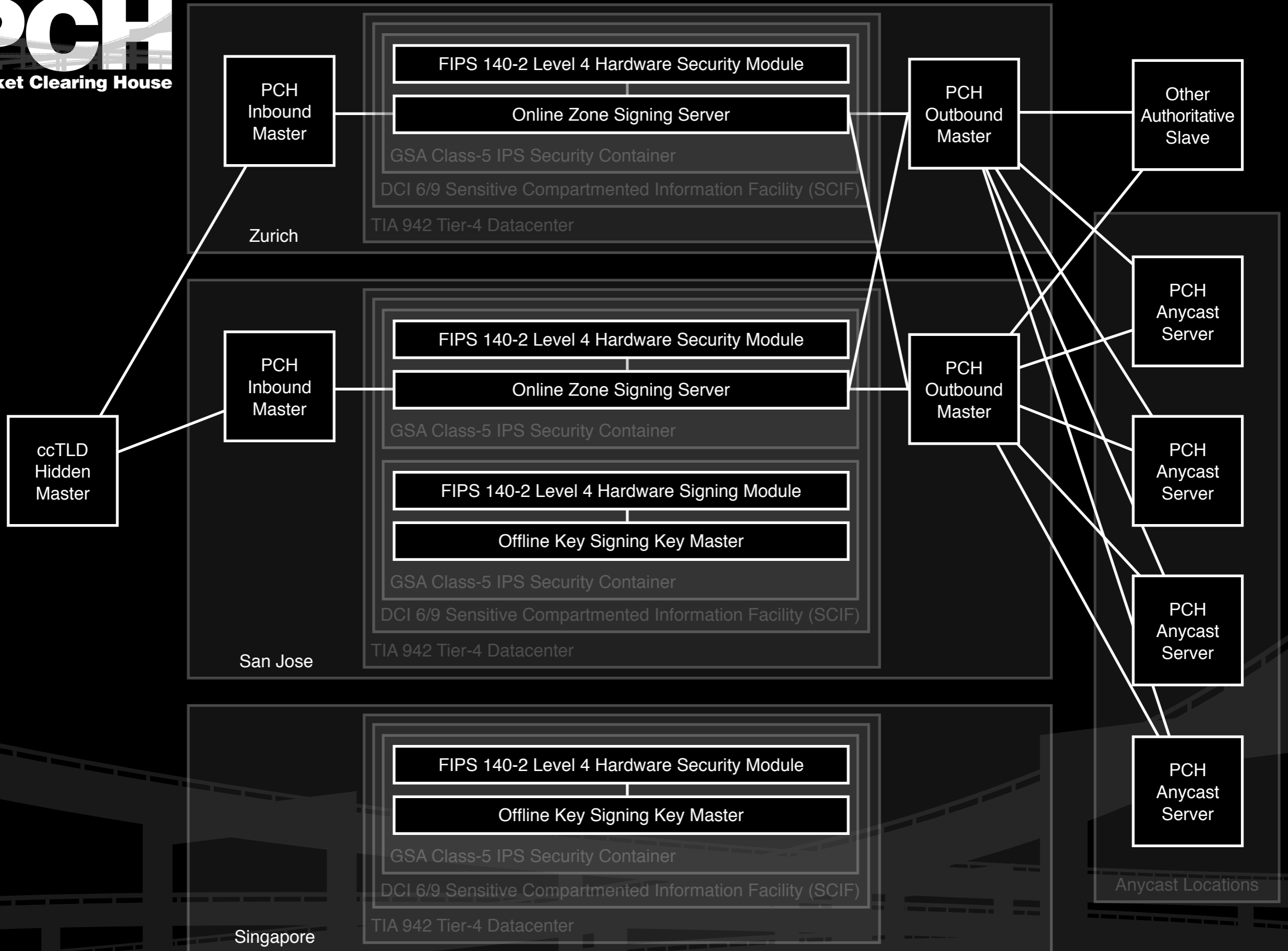Equinix Datacenter
Commercial

Europe
Zurich, Switzerland
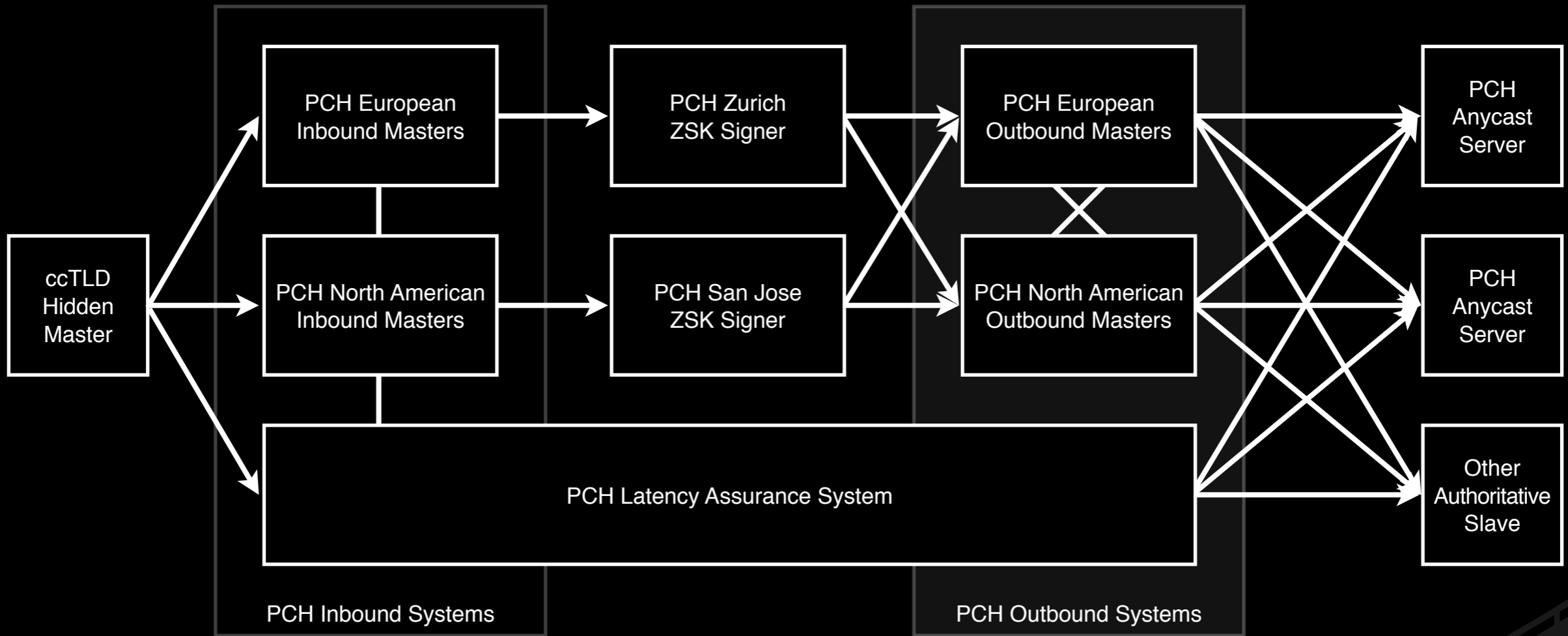SWITCH Datacenter
Research & Education

Asia-Pacific
Singapore
National University Datacenter
Research & Education

...With Integrated Global Anycast

PCH Inbound Master

FIPS 140-2 Level 4 Hardware Security Module

Online Zone Signing Server

GSA Class-5 IPS Security Container

DCI 6/9 Sensitive Compartmented Information Facility (SCIF)

TIA 942 Tier-4 Datacenter

Zurich

PCH Outbound Master

Other Authoritative Slave

ccTLD Hidden Master

PCH Inbound Master

FIPS 140-2 Level 4 Hardware Security Module

Online Zone Signing Server

GSA Class-5 IPS Security Container

FIPS 140-2 Level 4 Hardware Signing Module

Offline Key Signing Key Master

GSA Class-5 IPS Security Container

DCI 6/9 Sensitive Compartmented Information Facility (SCIF)

TIA 942 Tier-4 Datacenter

San Jose

PCH Outbound Master

PCH Anycast Server

PCH Anycast Server

PCH Anycast Server

FIPS 140-2 Level 4 Hardware Security Module

Offline Key Signing Key Master

GSA Class-5 IPS Security Container

DCI 6/9 Sensitive Compartmented Information Facility (SCIF)

TIA 942 Tier-4 Datacenter

Singapore

PCH Anycast Server

Anycast Locations

Live Demo!

ccTLD Test Phases

1: Sign zone, verify validity on signing system

2: Sign zone, publish on anycast servers, verify distribution and public visibility

3: Coordinate authoritative slaves to pull signed zone

4: Put DS record in the root, go live

PCH
Packet Clearing House

Thanks, and Questions?

Copies of this presentation can be found
in Keynote, PDF, QuickTime and PowerPoint formats at:

http:// www.pch.net / resources / papers

Bill Woodcock
Research Director
Packet Clearing House
woody@pch.net