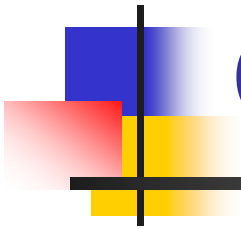
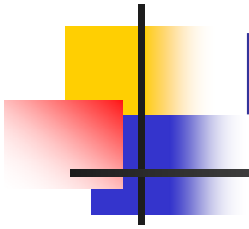


Signature-Only DNSSEC – A Quick Overview

Mike StJohns
stjohns@nominum.com
IETF67
http://www.ietf.org/internet-drafts/draft-stjohns-dnssec-sigonly-00.txt

Some Terms

- PNE – Provable Non-Existence DNSSEC; AKA – Authenticated Denial of Existence
- Sig Only or SO – Signature Only DNSSEC



PNE vs SO

- Most changes at validator, not at origin
- SO is PNE
  - Plus:
    - Off-tree Signatures
  - Minus
    - NSEC/NSEC3 Records (and supports)
    - Intermediate Validation
- Validation occurs ONLY at End-Client

What Does PNE Give Us?

		PNE Can Differentiate ↓	↓	
PNE	Secure	Bogus	Unsecure	Unknown
Sig Only	Validated	Unvalidated		

Output from Validation Algorithms

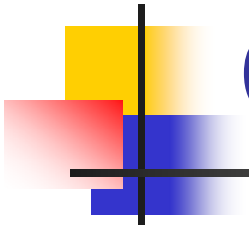
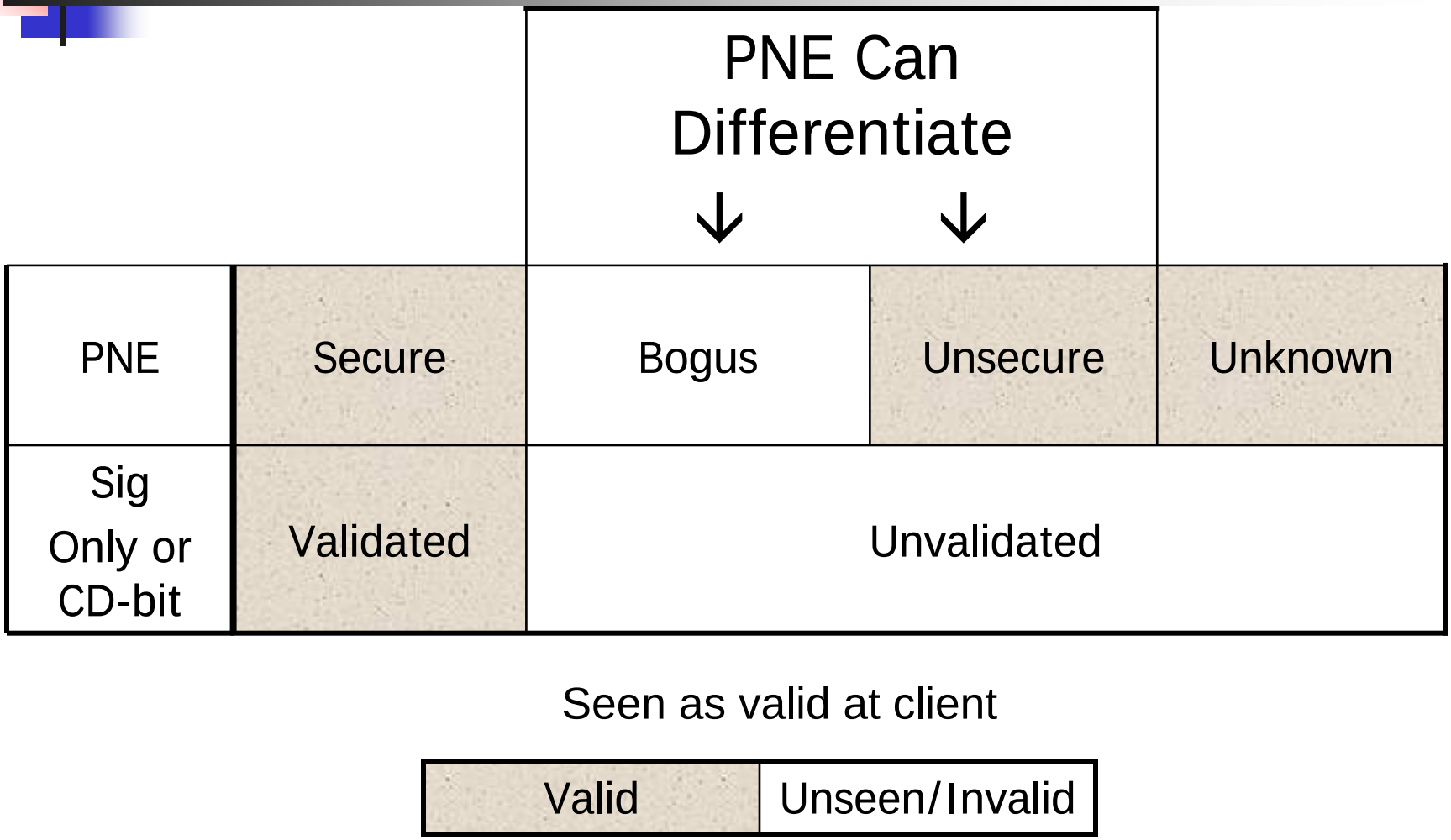


Chart Notes:

- RFC4033 “Indeterminate” output is undifferentiated from “Bogus” and is included there on previous slide
- “Unknown” refers to data with no superior trust anchor known by resolver
- If data can be validated then PNE doesn’t come into play (except perhaps wildcards) – e.g. PNE doesn’t differentiate Secure from any other state

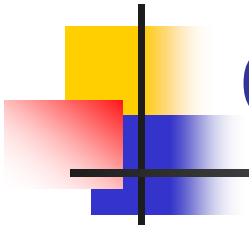
What Does the Client See?



What does PNE Cost?

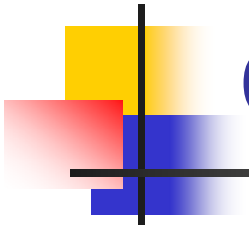
- NSEC and NSEC3 Records
- Monolithic zones – i.e. can't just add or delete an ownername or RR type under ownername
- Complex rules for what "MUST" be signed
- No off-tree signatures
- 13+ Years – and counting
- More fragile DNS (e.g. one error in signing can cause entire branch of tree to disappear from resolver POV)
- Complex validation algorithm for "Bogus" state

What can PNE do that SO can’t?



- Intermediate Resolver Validation
  - Feature or Mis-feature?
  - Does the “Site Finder” lesson apply?
- May have some wildcard limitations
  - Wildcard vs ownername covered by wildcard
- May be able to short-cut some lookups
  - PNE “knows when to stop”?

What can SO do that PNE can’t?



- Off-Tree signatures
- No intermediate validation requirement (e.g. simpler recursive server)
- Per-Application validation behavior (PNE can do this, but not core approach)

Protocol Differences

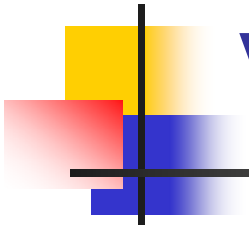
- Two New RR Types
  - DSSO – Same as DS except indicates delegation to an SO-only zone
  - OSIG – Off-tree Signature record; signature over single apex DNSKEY by key located somewhere else – e.g. other DNSKEY or public key certificate

Authoritative Server Changes

- DNSSEC special handling for DSSO record (i.e. same handling as DS) and OSIG (same as RRSIG(DNSKEY))
- PNE-capable Authoritative can do SO “leaf” zone (no further delegations) without changes (but may complain about lack of NSEC records)
  - OSIG use signaled by RRSIG(DNSKEY) RR with special Algorithm type

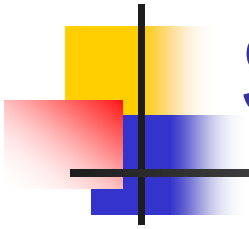
Recursive Server Changes

- Assumption: Server implements PNE
- Add DNSSEC special handling for DSSO and OSIG RR Types
- Client sets CD bit so…
  - Note: possible bug in RFC4035 – 3.2.2 – Shouldn't "client side of recursive server MUST copy setting of CD bit from the query to recursive queries" be included?



Validation Notes

- Chain of trust can flow through either SO or PNE zones – SO validator just ignores extraneous NSEC info
- No “downgrade” attacks – validator specifies set of minimally acceptable algorithms



Summary

- Simpler zone management
- Mostly backwards compatible with existing server software
- More work for client
  - But client gets most of the benefit!