DANE WG Issues Status
IETF 82, Taiwan

Richard Barnes
Paul Hoffman
Jakob Schlyter

What will be covered today

- Recently closed issues
- Currently open issues and proposed resolutions

Issue #23: DANE exclusivity

- Request: Use DANE to assert that no TLS services exist at the specified host and port
  - Exclusivity for a specific domain name
  - Exclusivity for a broader class of domain names
- Observation: Separate use case, could be done with a new usage type
- Proposed actions: Defer to a separate document
  - That is, nothing for now

Issue #37: Additive assertion of a server certificate

- Request: Add a usage to assert a self-signed server certificate directly, instead of a CA certificate that could be used to verify the server cert
- Proposed resolution: None
  - Covered by usage 2 (TA assertion)

Issue #38: EAP-FAST

- Request: Enable support for DANE within EAP-FAST
- Proposed action: None
  - EAP-FAST uses TLS over various protocols (e.g., RADIUS/Diameter, PPP, IKE), so normal DANE procedures apply
  - Separate document specifying DANE for EAP might be needed to clarify how domain name mapping should be used
    - e.g., SSID to domain name
  - Should be done by EAP-FAST developers, not DANE WG

Issue #8: The last mile problem

- Request: In order to use DANE with high assurance, clients need access to DNSSEC validation information
  - Perform validation locally, or
  - Use a trusted resolver over a secure channel
- Proposed action: Add a paragraph to security considerations to note this

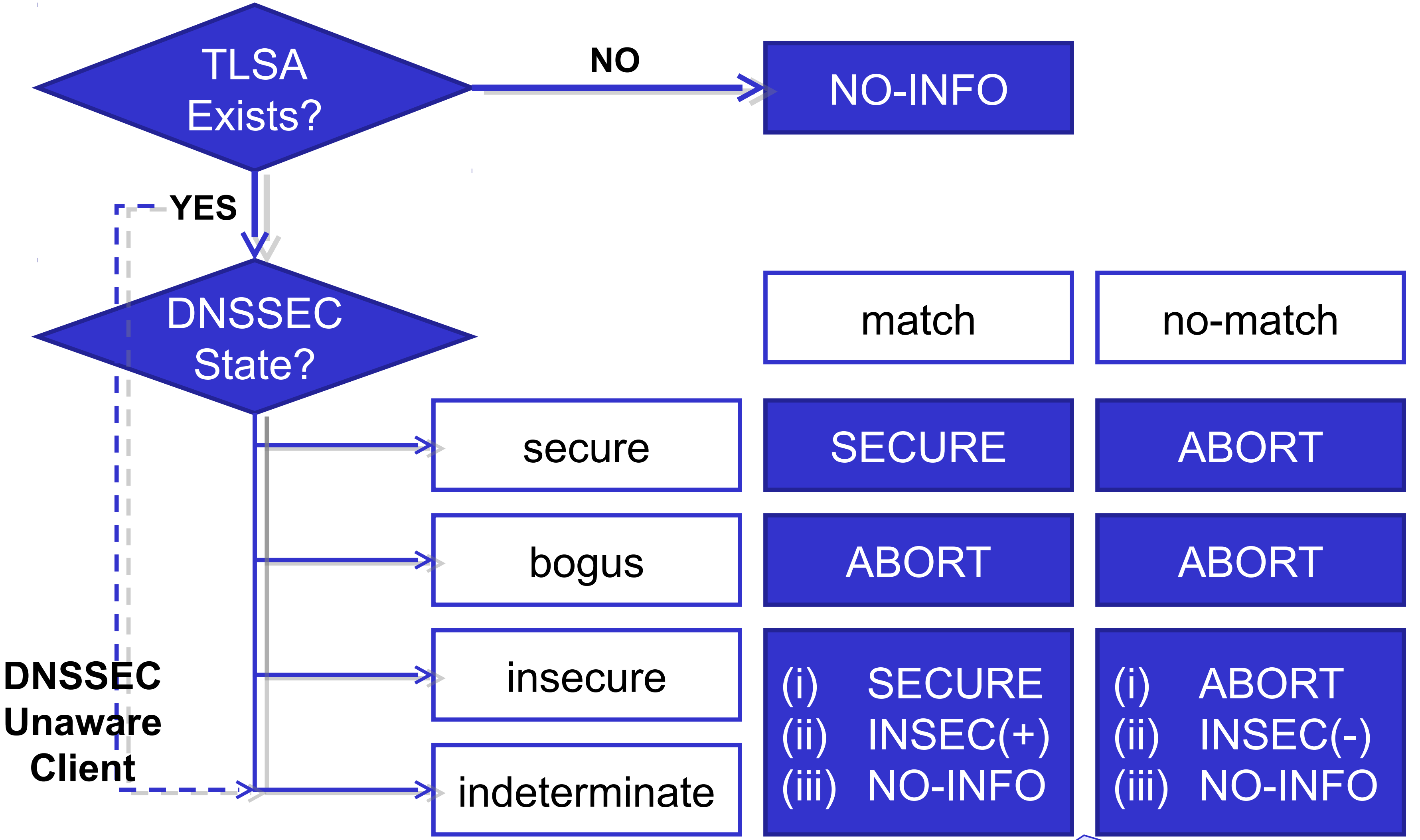
Issue #10: Compromise of an Intermediate CA

- Request: Note that DANE could conflict with PKIX information about intermediate CAs
    - Domain adds TA assertion for intermediate CA
    - Superior CA revokes intermediate CA cert
    - DANE validators never see revocation
- Proposed action: Add a paragraph to the Security Considerations to note this

Issue #36: Only requiring DNSSEC where it is needed

- Request: Remove restriction that all TLSA records MUST have DNSSEC protection
- Proposed action: Add a "client processing" section that specifies behavior in all DNSSEC cases

DANE Decision Tree



	match	no-match
secure	SECURE	ABORT
bogus	ABORT	ABORT
insecure		
indeterminate	(i) SECURE (ii) INSEC(+) (iii) NO-INFO	(i) ABORT (ii) INSEC(-) (iii) NO-INFO

What should happen in these cases?
Different by usage type?

Summary of proposed actions

- No action:
  - Issue #23: DANE exclusivity
  - Issue #37: Assertion of server certificate
  - Issue #38: EAP-FAST
- Clarifying text for minor issues:
  - Issue #8: Last mile problem
  - Issue #10: Compromise of intermediate CA
- Add/Re-write "client processing" section
  - Issue #36: Only requiring DNSSEC where needed