Documenting and Managing Algorithm Lifecycles

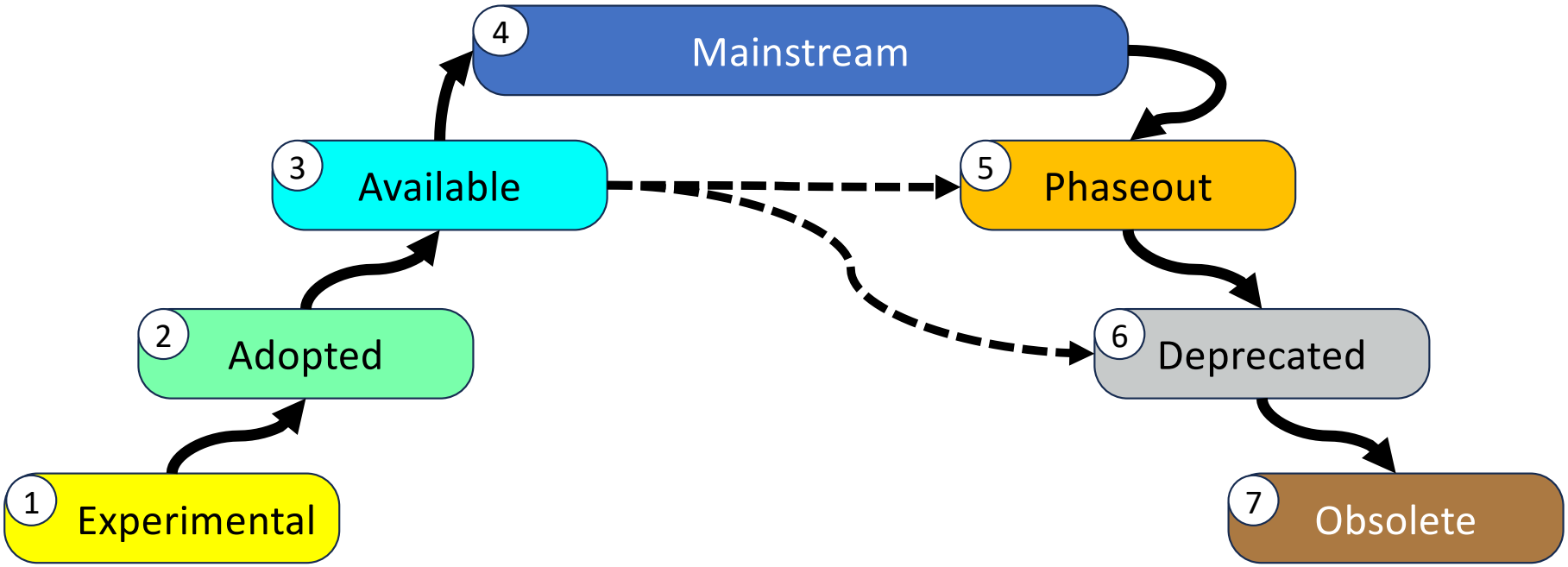
Steve Crocker, Russ Housley

25 October 2023

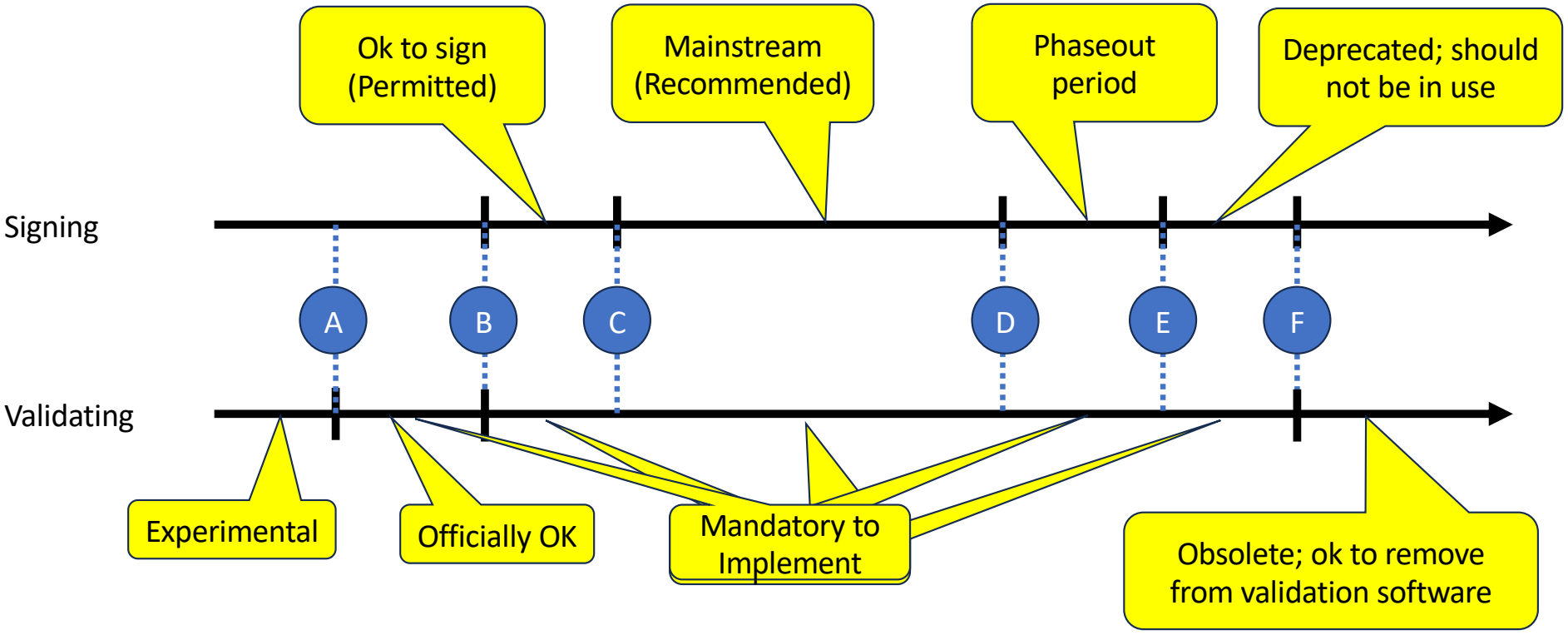
Summary

- These slides are intended to illustrate the lifecycle for DNSSEC signing algorithms. (The same ideas are applicable to other crypto algorithms.)
- It's well understood that an algorithm must be included in the validation software before it can be used for signing.
- And it's equally well understood that it cannot be removed from the validation software until signers have stopped using it.
- Included here is explicit treatment of the transition periods.
- These slides are intended for comment and discussion.

The Seven Phase in an Algorithm Lifecycle



The Six Transitions in an Algorithm Lifecycle



Transition Points

A: Prior to this time, usage is experimental. From this time onward, the algorithm should start to be included in validation software.

B: After this time, the algorithm is expected to be included in all validation software. Signers can begin to use the algorithm.

C: After this point, the algorithm is considered mainstream.

D: At this point, the algorithm is declared to be reaching its end of life. Signers are advised to begin transitioning to a new algorithm, and to do so by an estimated date (e).

E: Signers must not use the algorithm after this time, but validators must continue recognizing and validating.

F: After this point the algorithm is considered obsolete. Validators no longer need to recognize and validate.

Phases

1. Experimental (prior to A)
2. Adopted (between A and B) – begin inclusion in validation suite
3. Available (between B and C) – ok to use for signing
4. Mainstream (between C and D) – recommended for signing
5. Phaseout (between D and E) – transition to newer signing algorithm
6. Deprecated (between E and F) – signing should have stopped
7. Obsolete (after F) – ok to remove from validation suite

Proposed Event Criteria

A. Algorithm Inclusion

- Prerequisites:
  - Algorithm has been given a name and IANA designation
  - Crypto community has blessed the algorithm as suitable to use.
  - Documentation and implementations exist and deemed reliable
- IETF determines the algorithm is suitable for use
- Action: IETF publishes notice that the algorithm is suitable for use and should be deployed in all validation suites.

B. Ready for use

- Prerequisites:
  - Deployment has been measured
  - Deployment has reached an acceptable level
- IETF reaches consensus that algorithm has been fully deployed
- Action: IETF publishes notice that algorithm is available for signing.

C. Mainstream

- IETF reaches consensus that algorithm has reached mainstream status
- Actions:
  - IETF publishes notice that algorithm has reached mainstream status.
  - Signers using older algorithms, particularly algorithms in the Phaseout or later phases should transition to a mainstream algorithm.

D. Phaseout

- Prerequisites:
  - Crypto community has determined the algorithm is reaching its end of life.
- IETF determines it's time to announce the phaseout
- Action: IETF publishes notice to signing operators to transition away from this algorithm and begin signing with a mainstream algorithm.

E. Deprecation

- Prerequisites:
  - Measure signing activity
  - Signing activity has subsided to minimal level
- IETF determines it's time to deprecate
- Action: IETF publishes notice that use of this algorithm for signing is inappropriate.

F. Obsolescence

- Prerequisite: Measurement of signing determines actual use has fallen to lowest achievable level
- IETF determines the algorithm is obsolete.
- Action: IETF publishes notice that algorithm is obsolete and may be removed from the validation suite.

Comparison with RFC 8624

RFC 8624, section 3.1, DNSKEY Algorithms

#	Mnemonics	Signing	Validation	Phase
1	RSAMD5	MUST NOT	MUST NOT	7
3	DSA	MUST NOT	MUST NOT	7
5	RSASHA1	NOT RECOMMENDED	MUST	6
6	DSA-NSEC3-SHA1	MUST NOT	MUST NOT	7
7	RSASHA1-NSEC3-SHA1	NOT RECOMMENDED	MUST	5
8	RSASHA256	MUST	MUST	3
10	RSASHA512	NOT RECOMMENDED	MUST	5
12	ECC-GOST	MUST NOT	MAY	6
13	ECDSAP256SHA256	MUST	MUST	3
14	ECDSAP384SHA384	MAY	RECOMMENDED	2?
15	ED25519	RECOMMENDED	RECOMMENDED	4
16	ED448	MAY	RECOMMENDED	3

This is an attempt to reconcile the table in RFC 8624, section 3.1. with the phases described in this briefing.

It isn't clear to me that the correspondences are correct.

Mapping RFC 8624 to these phases

		Signing				
		May	Must	Recommended	Not Recommended	Must Not
Validation	Recommended	2?		4		
	Must	3			5	
	May					6
	Must Not					7

A further attempt to reconcile the states in 8624 with the phases in this briefing.

Thanks and Follow-Up

- Feedback, guidance, etc. welcome
- If there is a natural home for this, or if this is already under control, that's great. Otherwise I remain interested.
- Thanks!

Steve@shinkuro.com