The Reality of Algorithm Agility: Studying the DNSSEC Algorithm Life-Cycle

DNSSEC and Security Workshop - ICANN69 Virtual Meeting, 21 October 2020

Moritz Müller[3,4], Willem Toorop[1], Taejoong Chung[2], Jelte Jansen[3], Roland van Rijswijk-Deij[1,4]

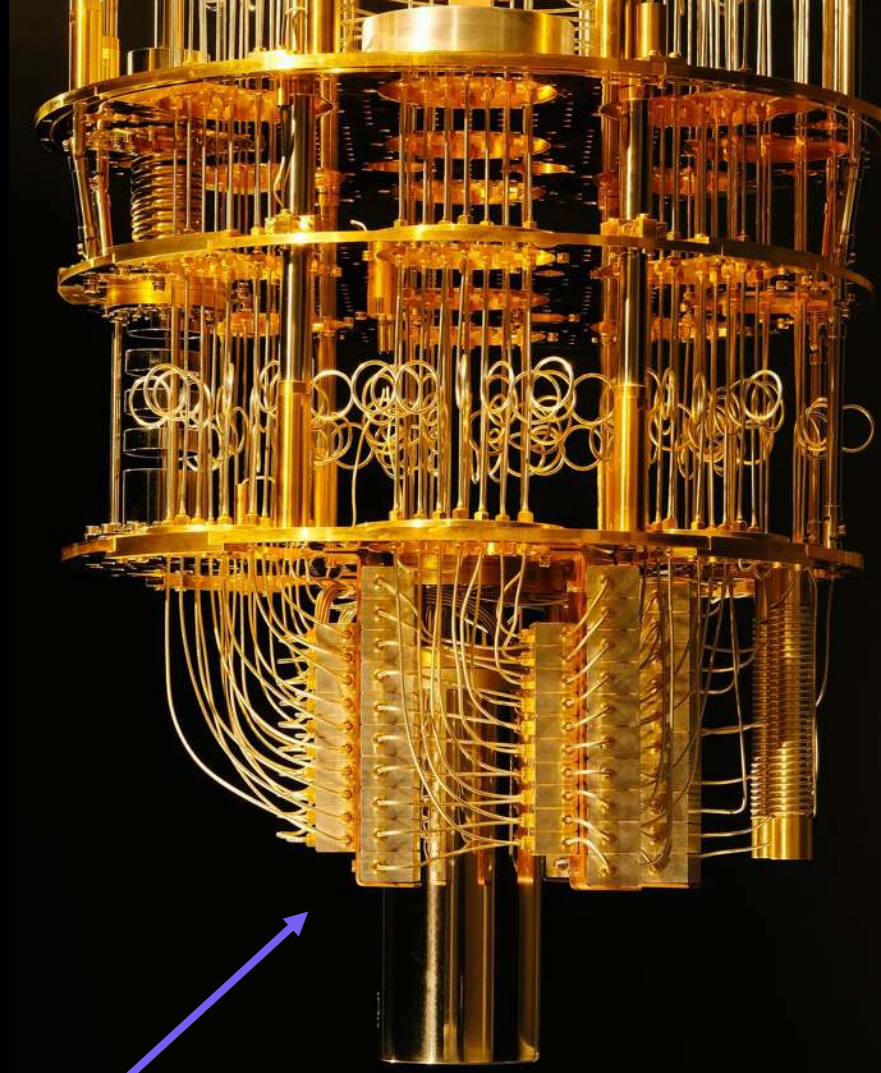
[1]NLnet Labs, [2]Virginia Tech, [3]SIDN Labs, [4]University of Twente

Introduction

- DNSSEC brings **integrity** to the DNS
- Heavily relies on the security of its signing algorithms
- Signing algorithms are added and removed because of:
  - Security
  - Performance

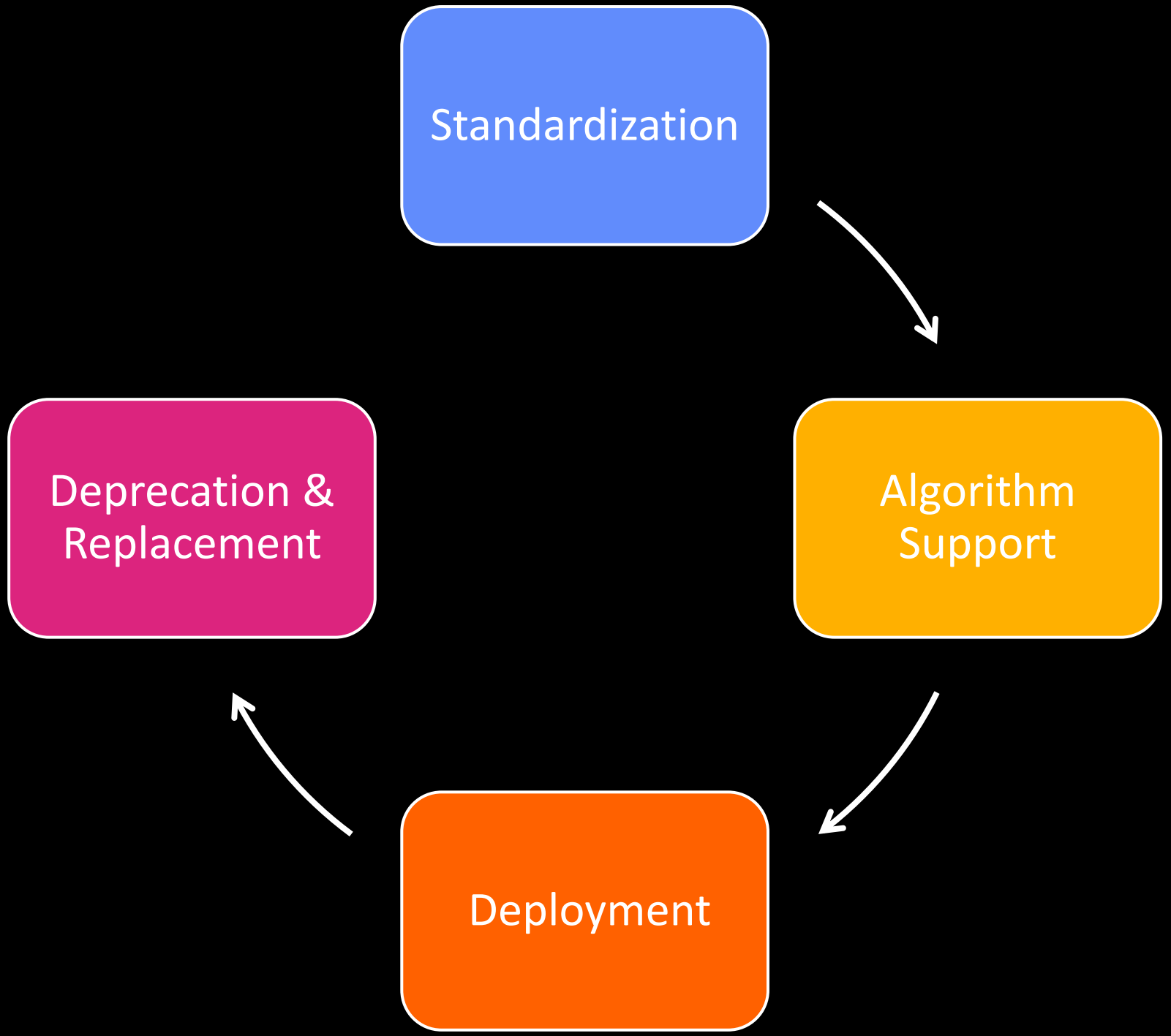
Introduction

- DNSSEC brings **integrity** to the DNS
- Heavily relies on the security of its signing algorithms
- Signing algorithms are added and removed because of:
  - Security
  - Performance
- Quantum computers might **render** all current algorithms **insecure**



Not a quantum computer, only its fridge

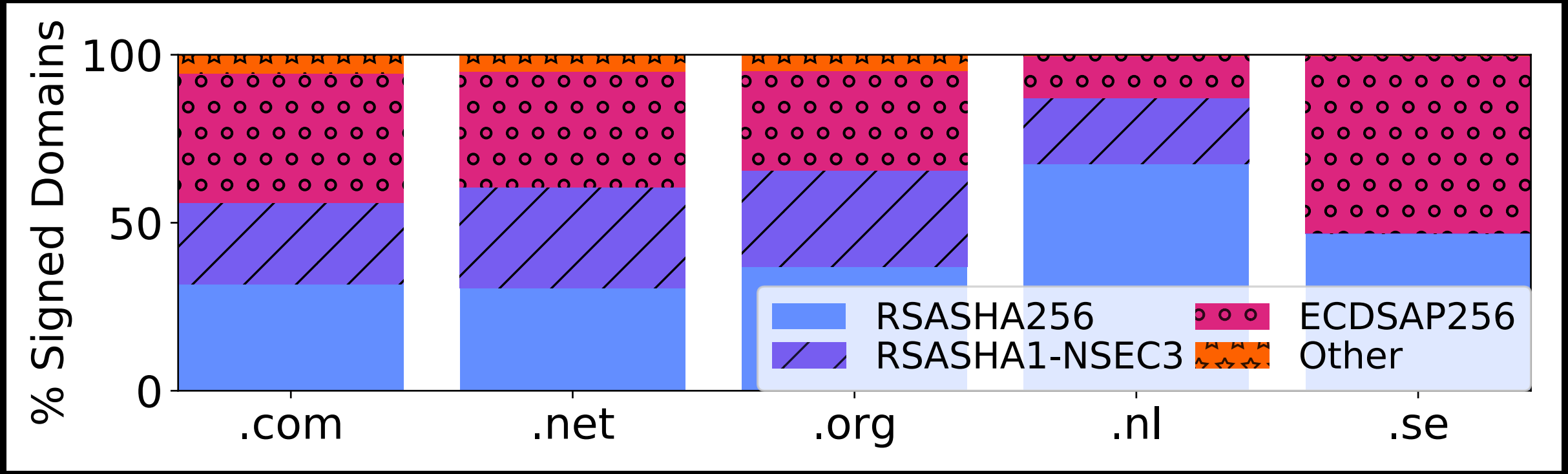
Algorithm Lifecycle

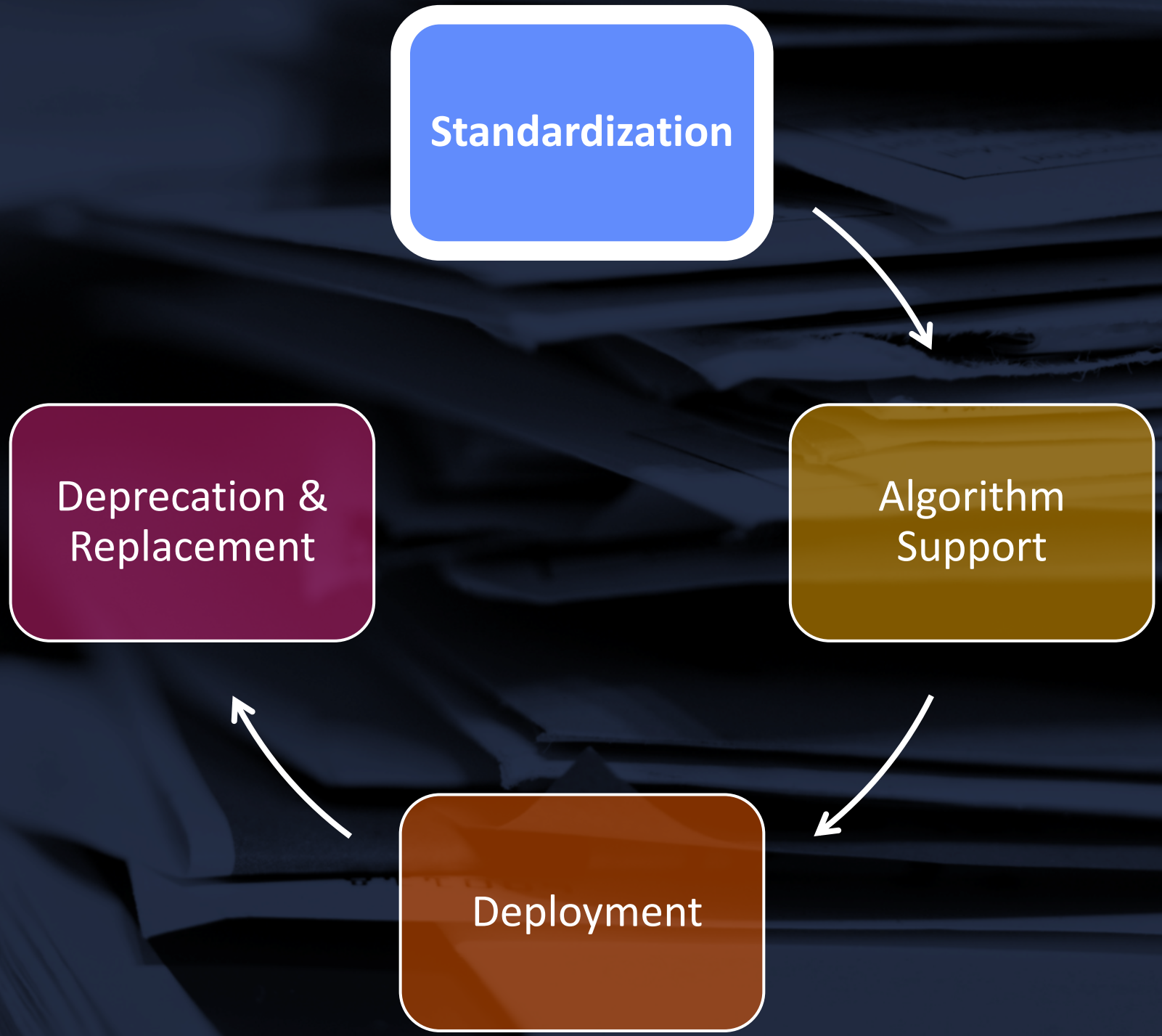


Analyzed Algorithms

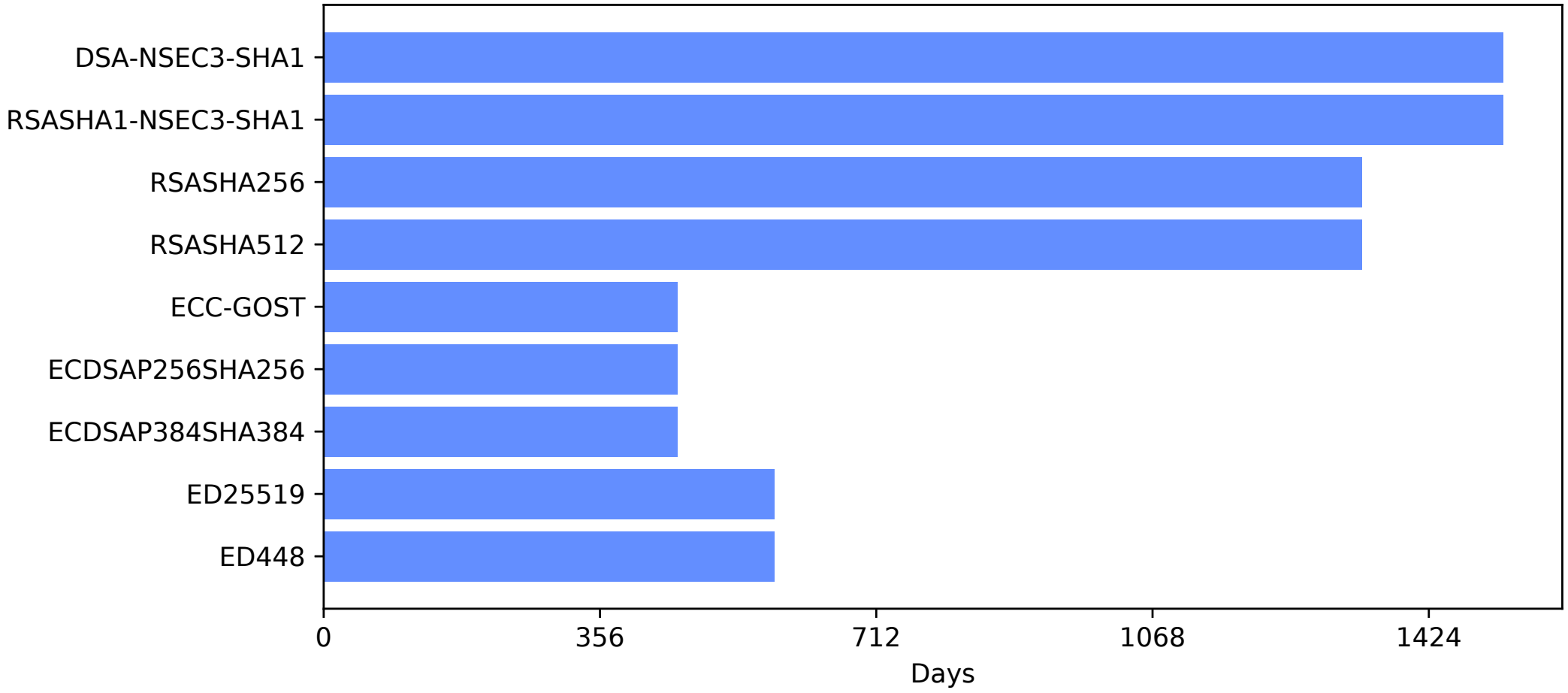
- **Standardization:** all algorithms
- **Algorithm Support:** all algorithms
- **Deployment:**
  - ECDSAP256 (signing)
  - ED25519 and ED448 (validation)
- **Deprecation:**
  - RSASHA-1-NSEC3-SHA1 (signing)
  - RSASHA-1-NSEC3-SHA1, DSA, RSASHA1, DSA-NSEC3-SHA1 (validation)

Currently Deployed Algorithms

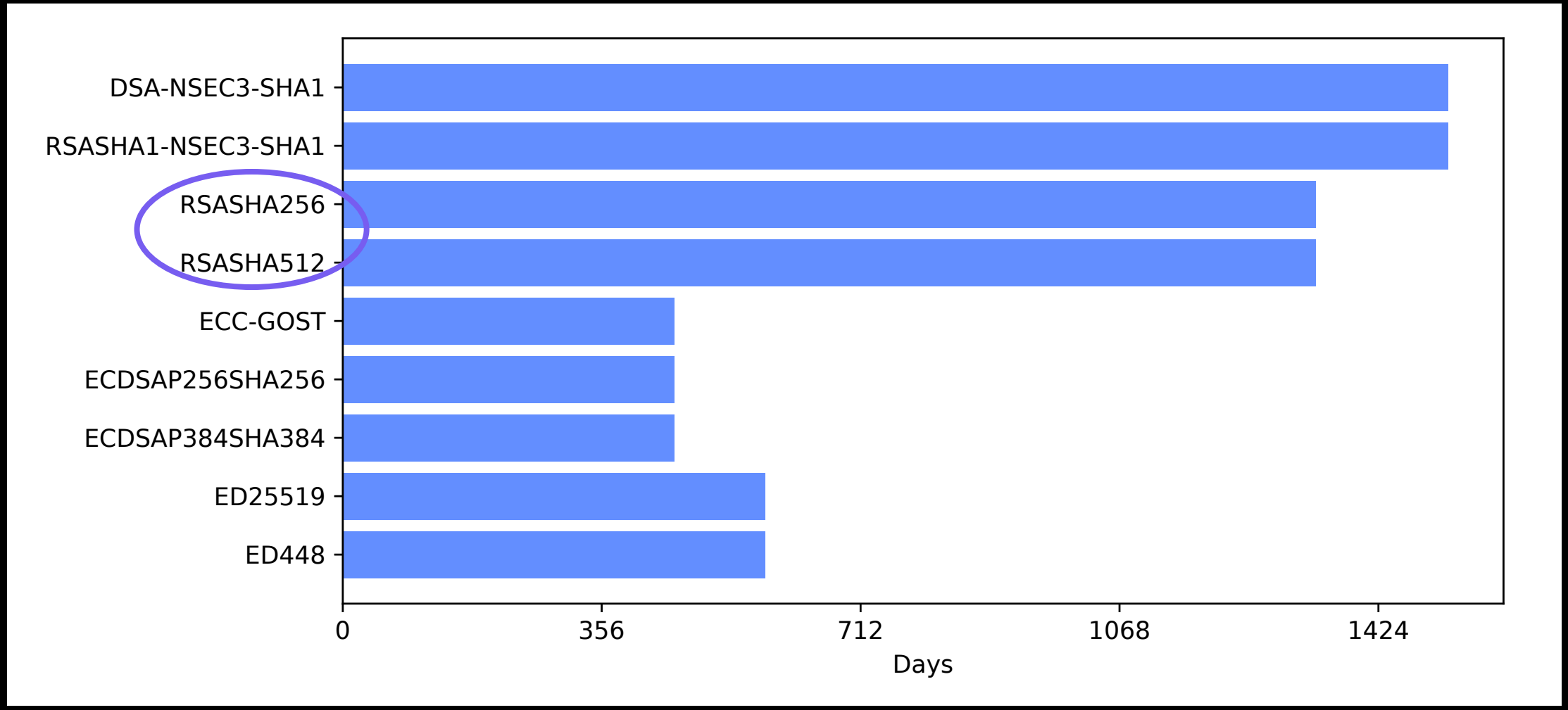


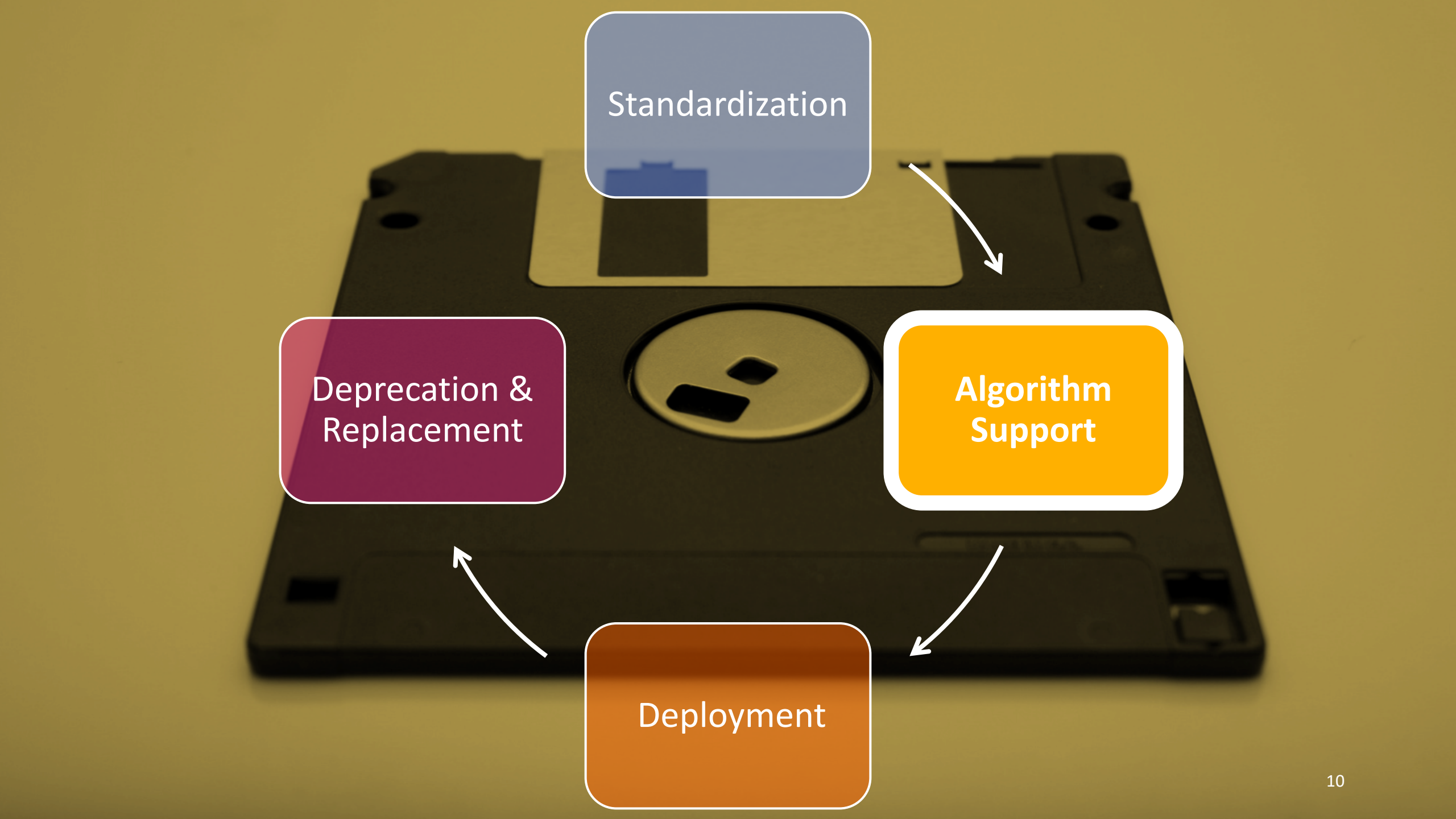

Standardization
Algorithm Support
Deployment
Deprecation & Replacement

Time until Standardization

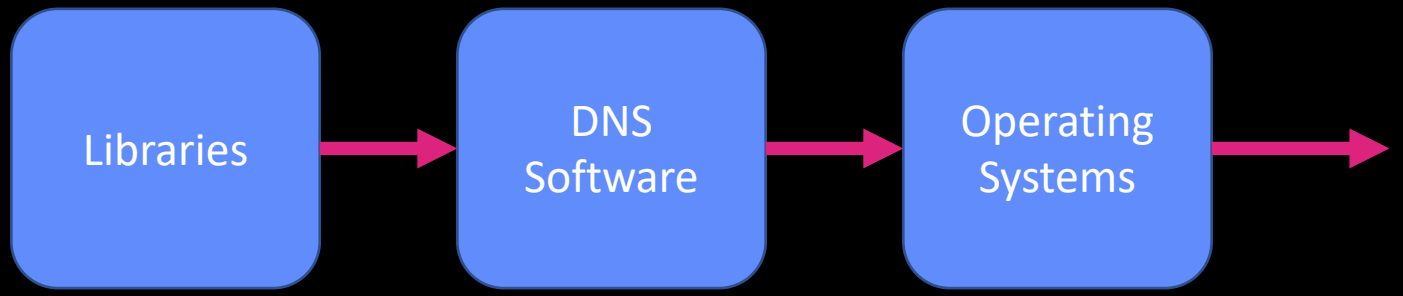


Time until Standardization




Standardization
Algorithm Support
Deployment
Deprecation & Replacement

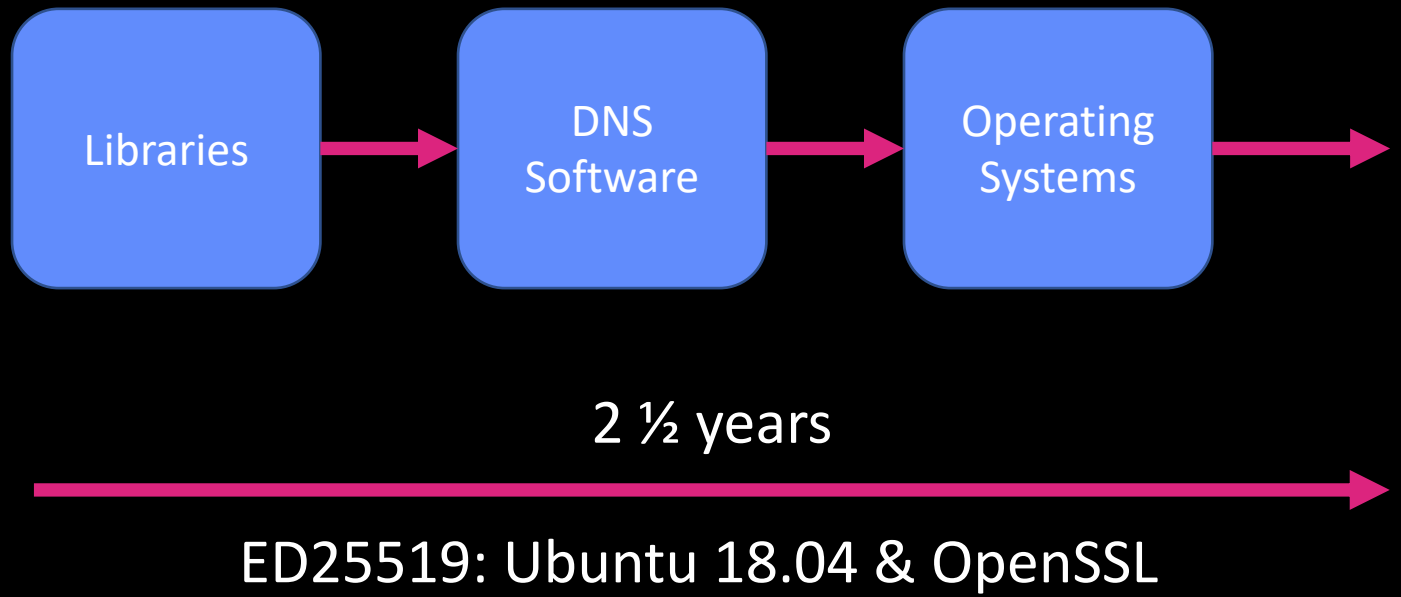
Path to Full Support



Ready for Deployment

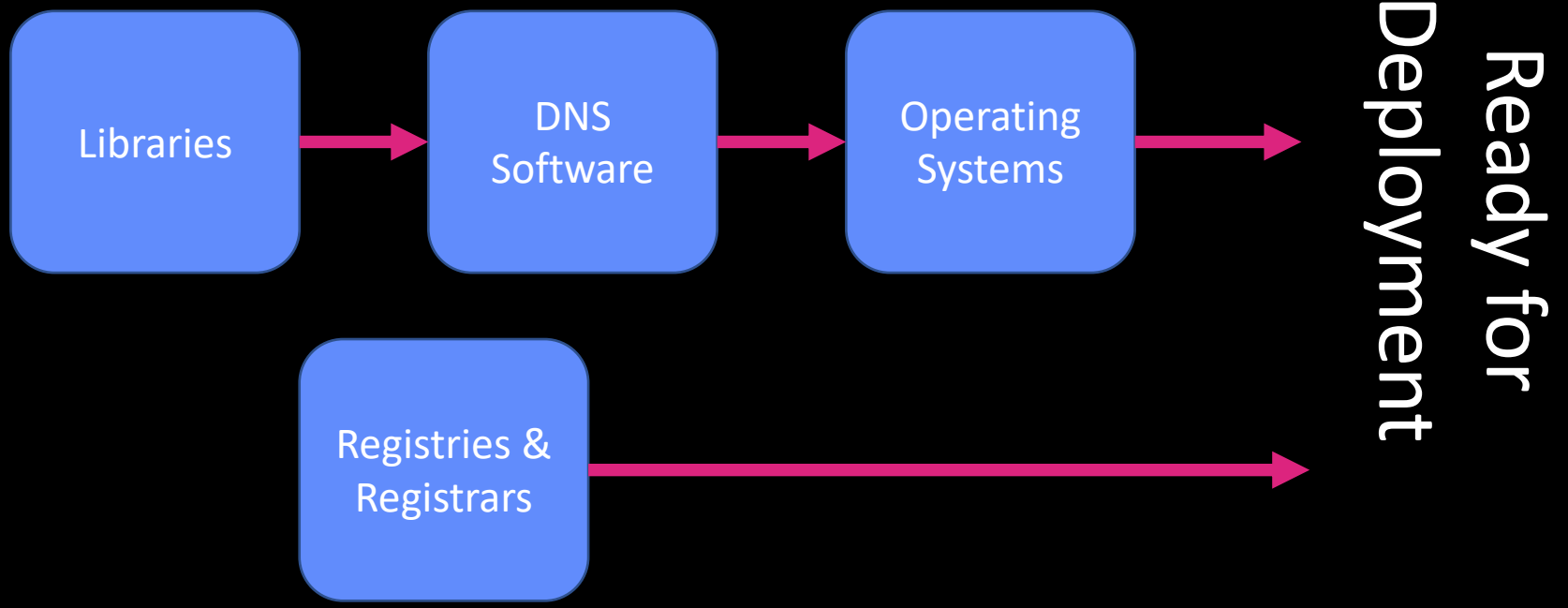
Photo by Josiah Farrow on Unsplash

Path to Full Support

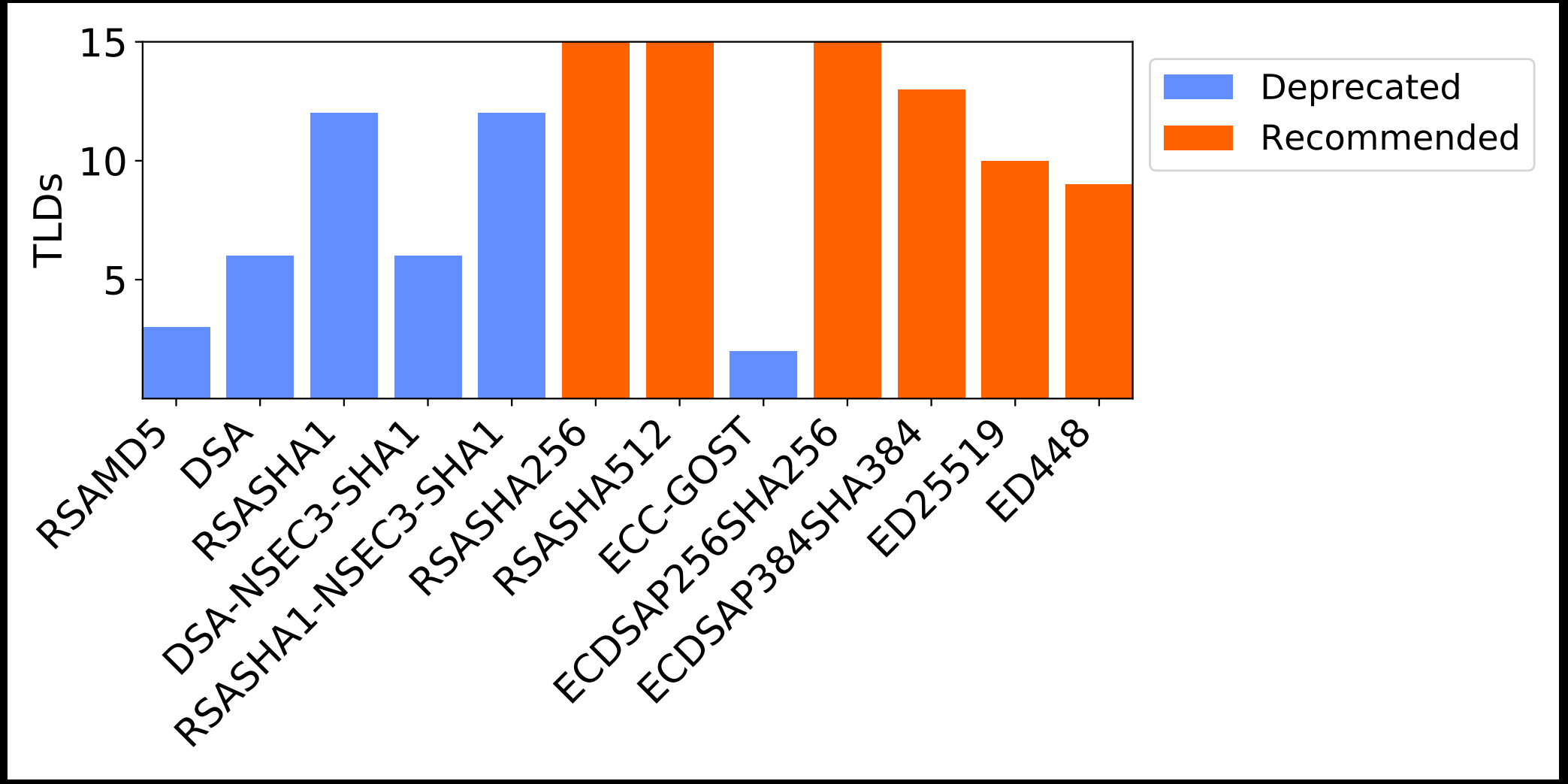


Ready for Deployment

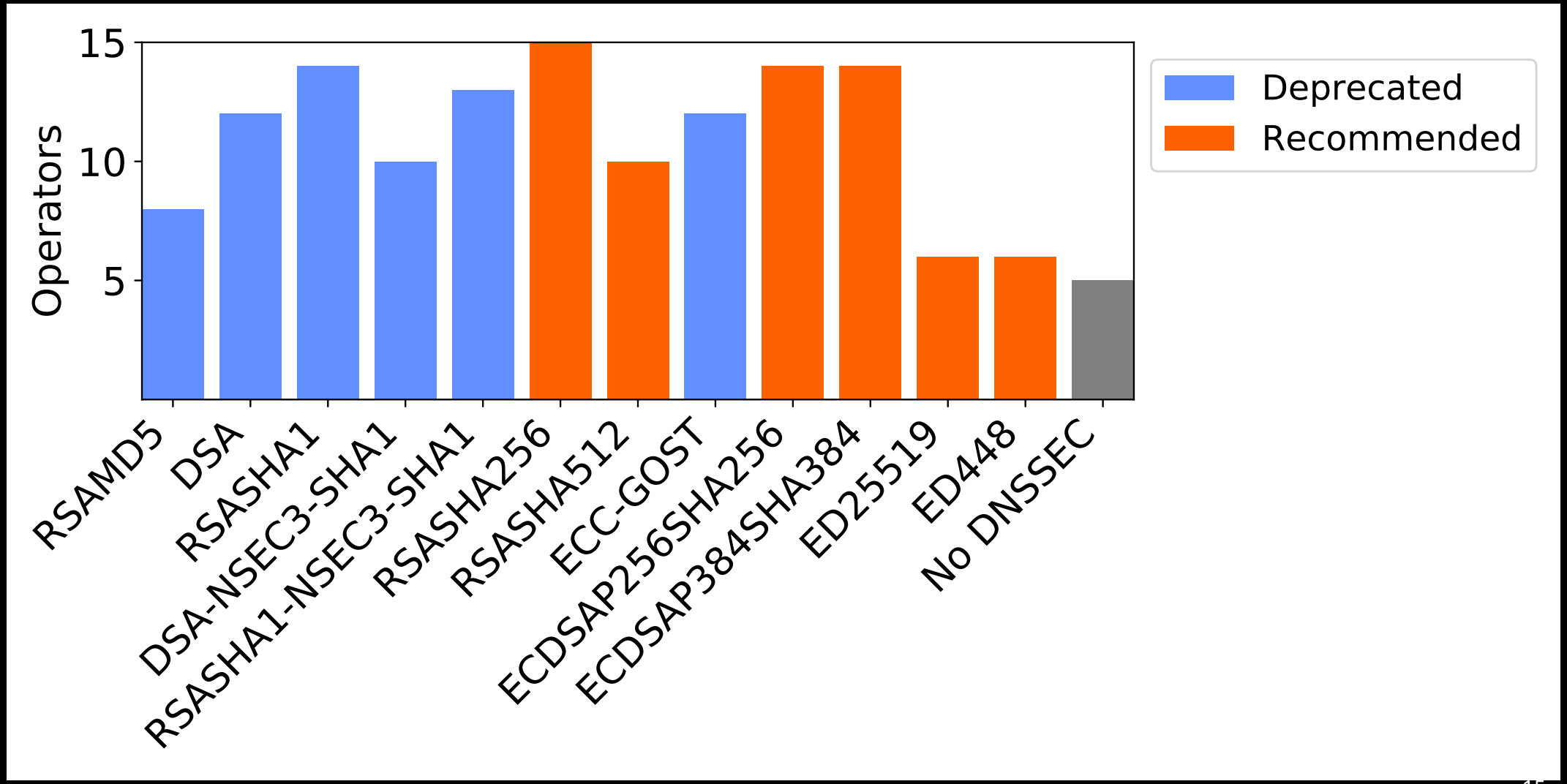
Path to Full Support

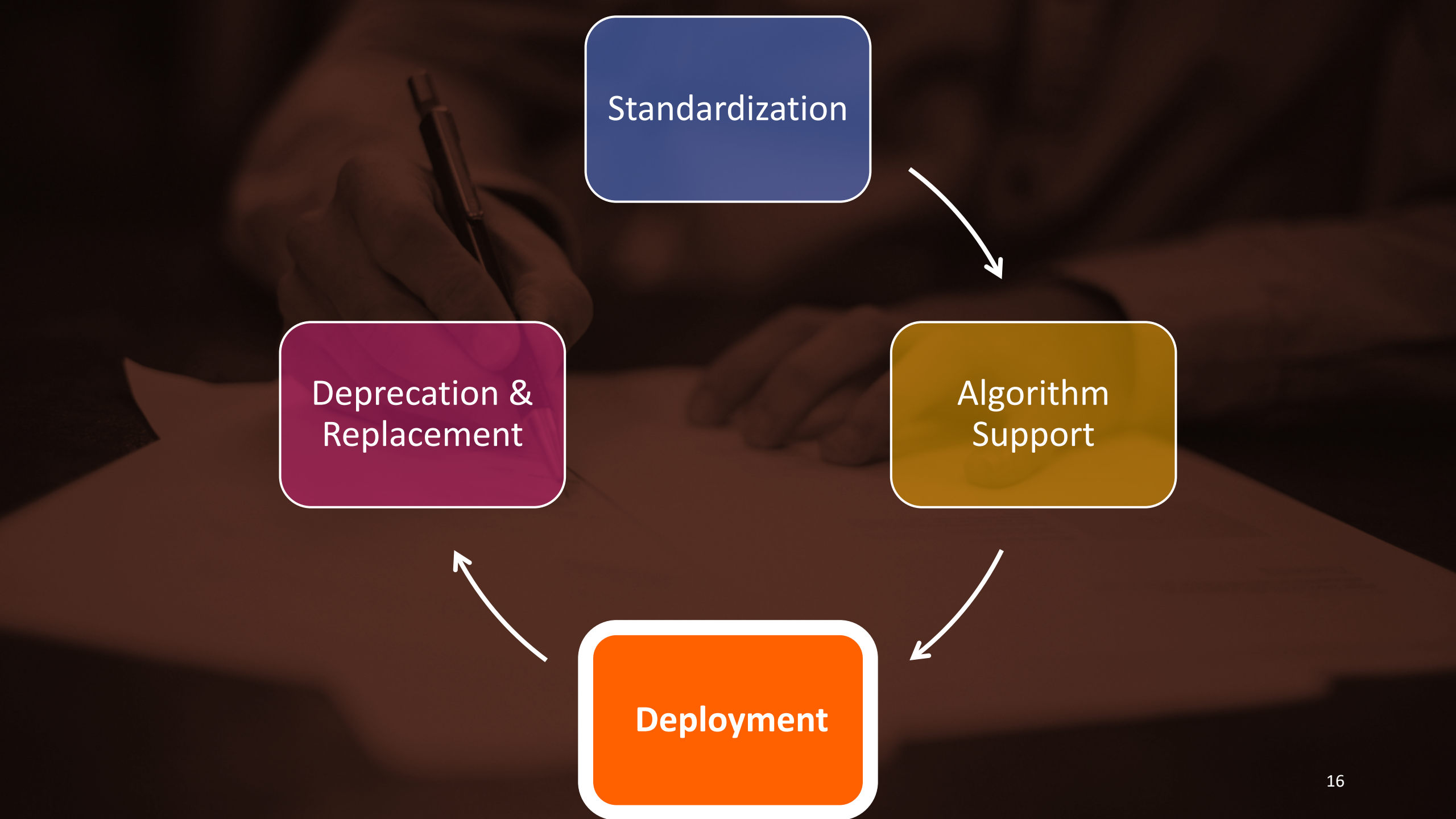


Registry Support

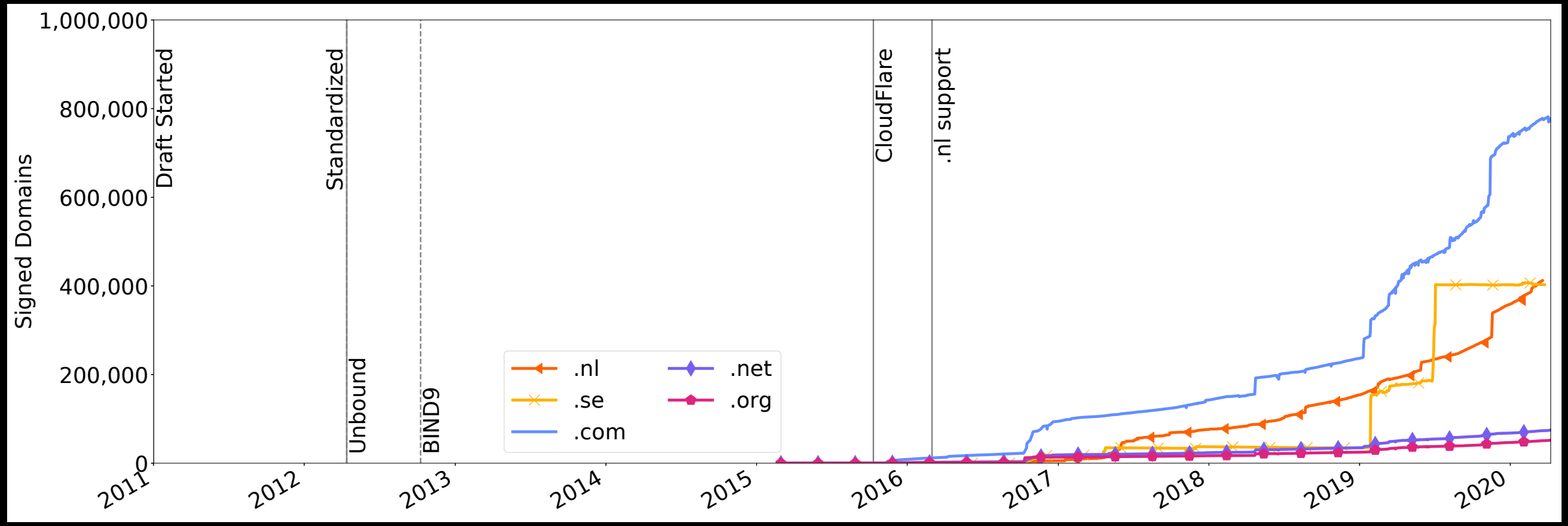


Registrar Support



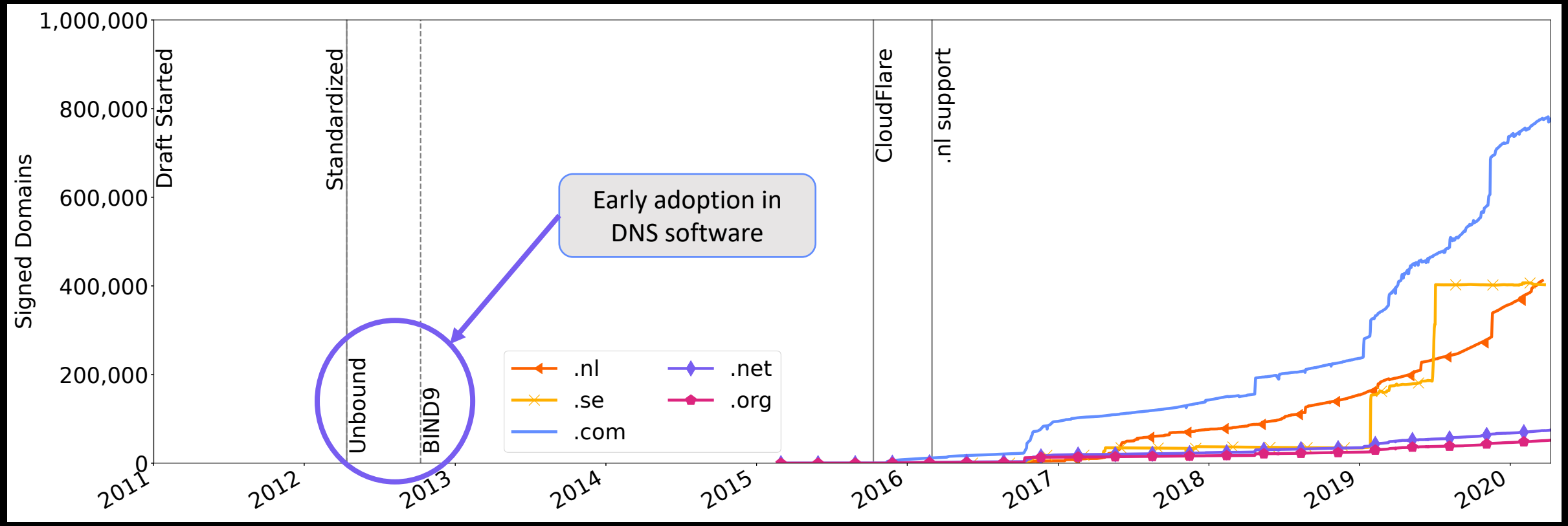

Standardization
Algorithm Support
Deployment
Deprecation & Replacement

Algorithm Deployment at Domain Names



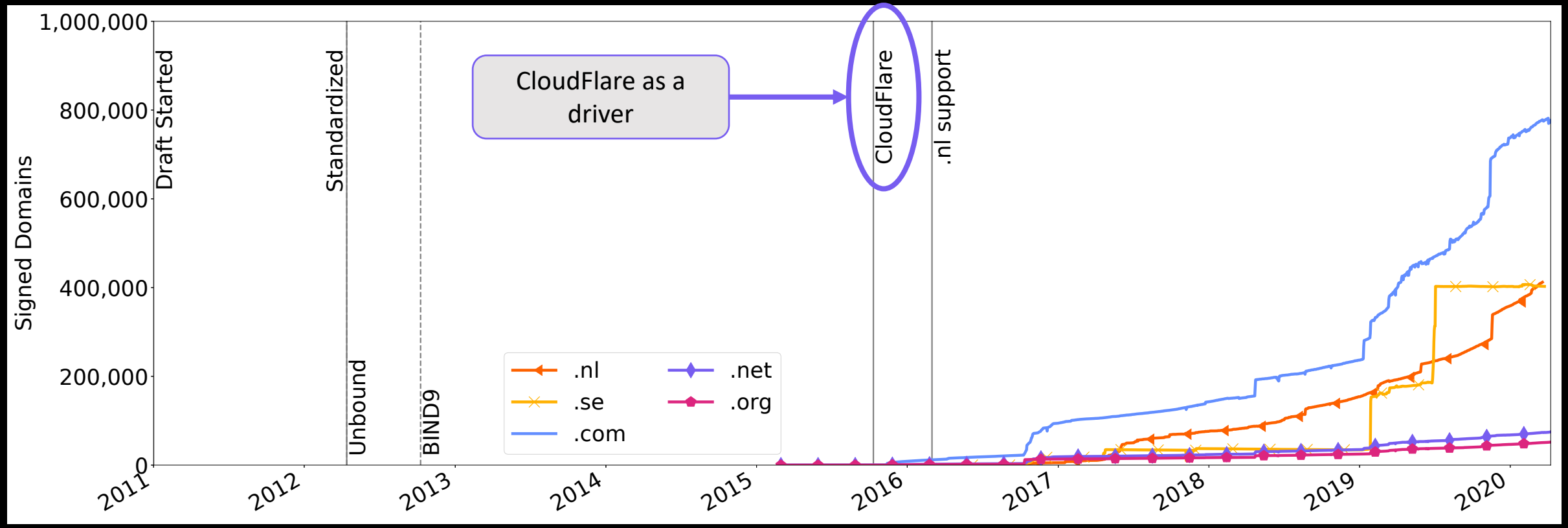
ECDSA256

Algorithm Deployment at Domain Names



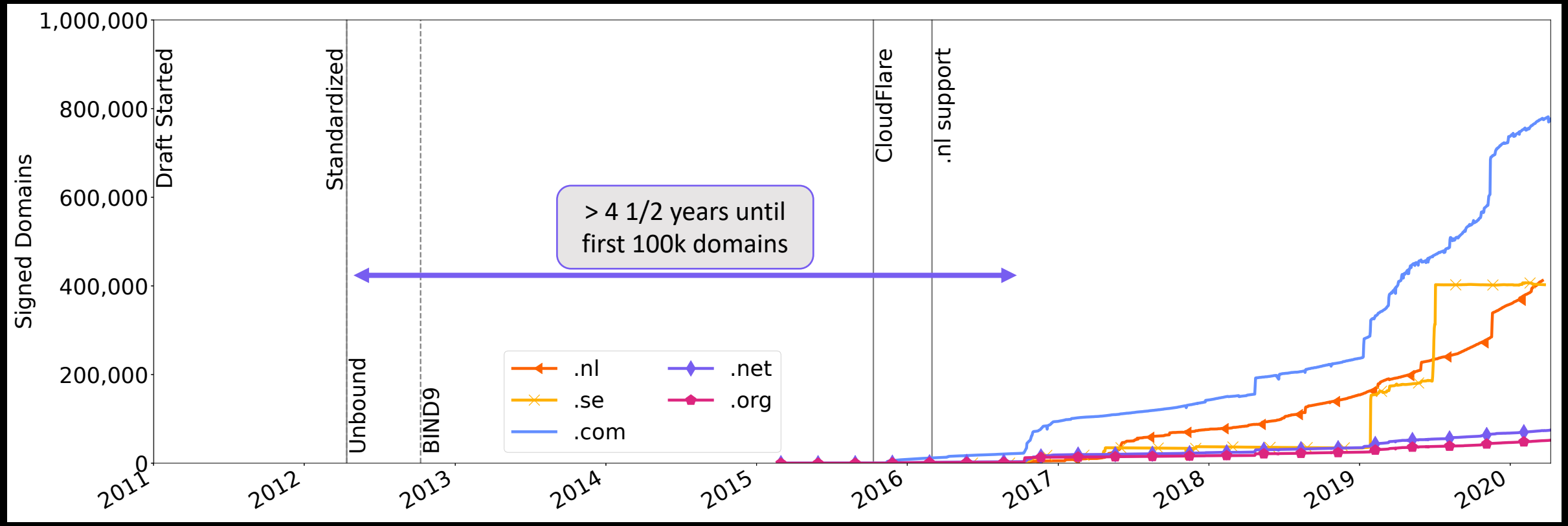
ECDSA256

Algorithm Deployment at Domain Names



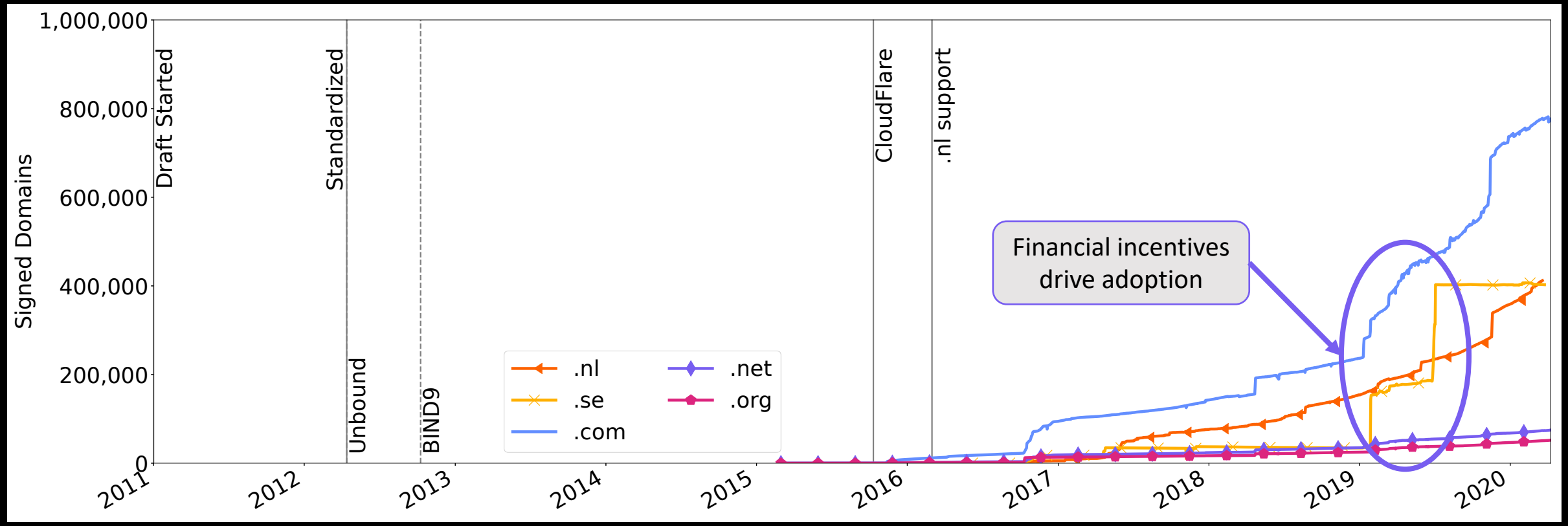
ECDSA256

Algorithm Deployment at Domain Names



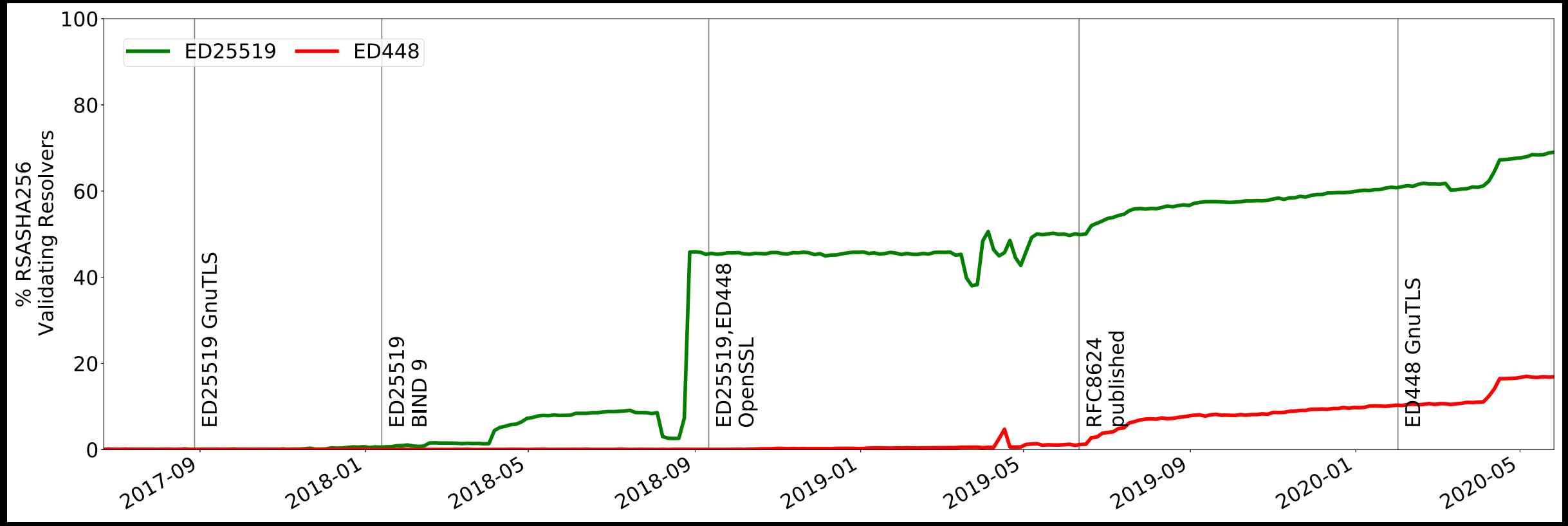
ECDSA256

Algorithm Deployment at Domain Names

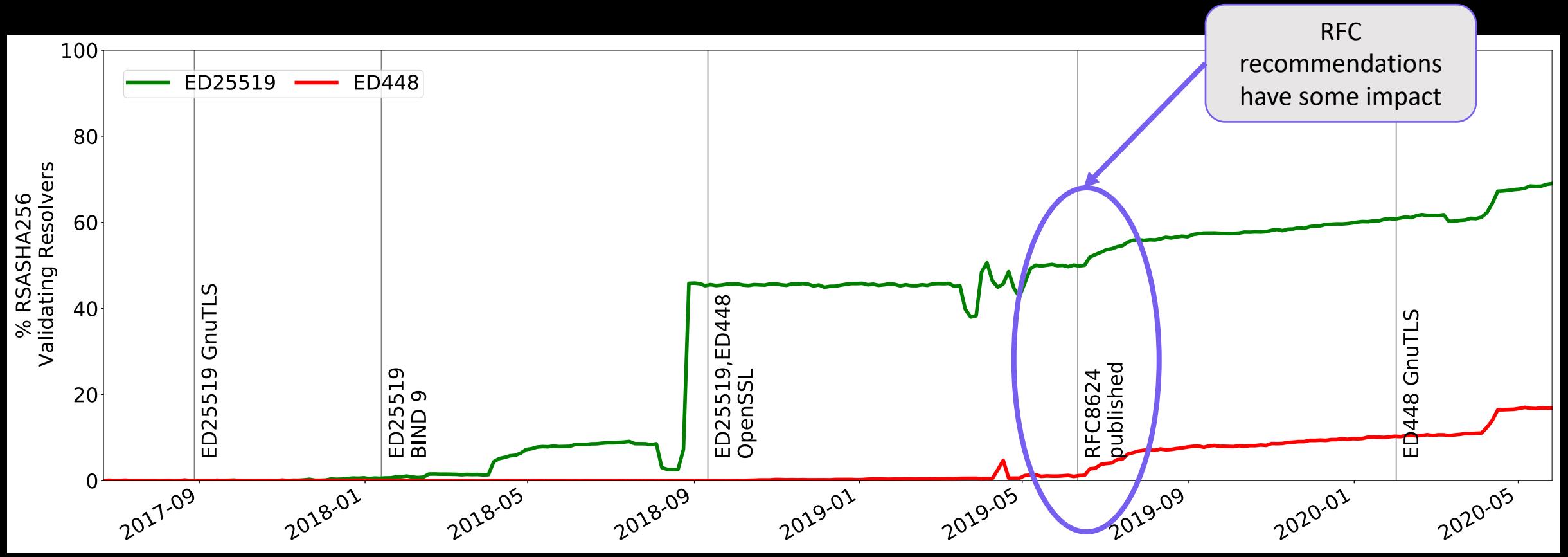


ECDSA256

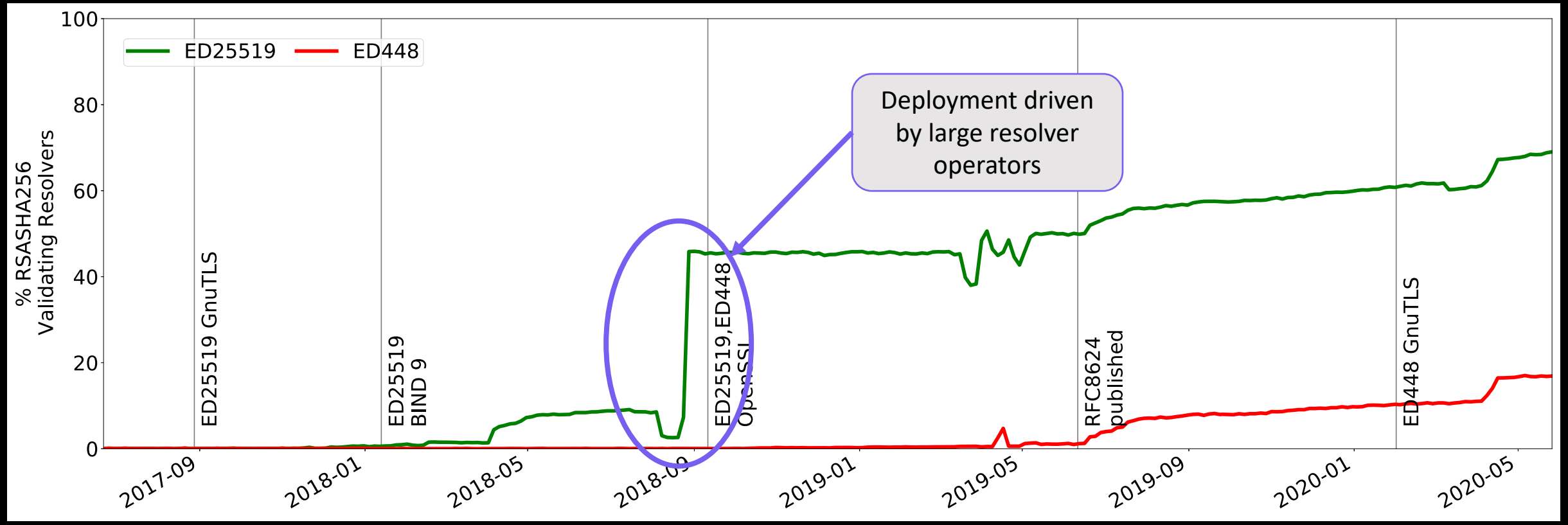
Algorithm Deployment at Resolvers

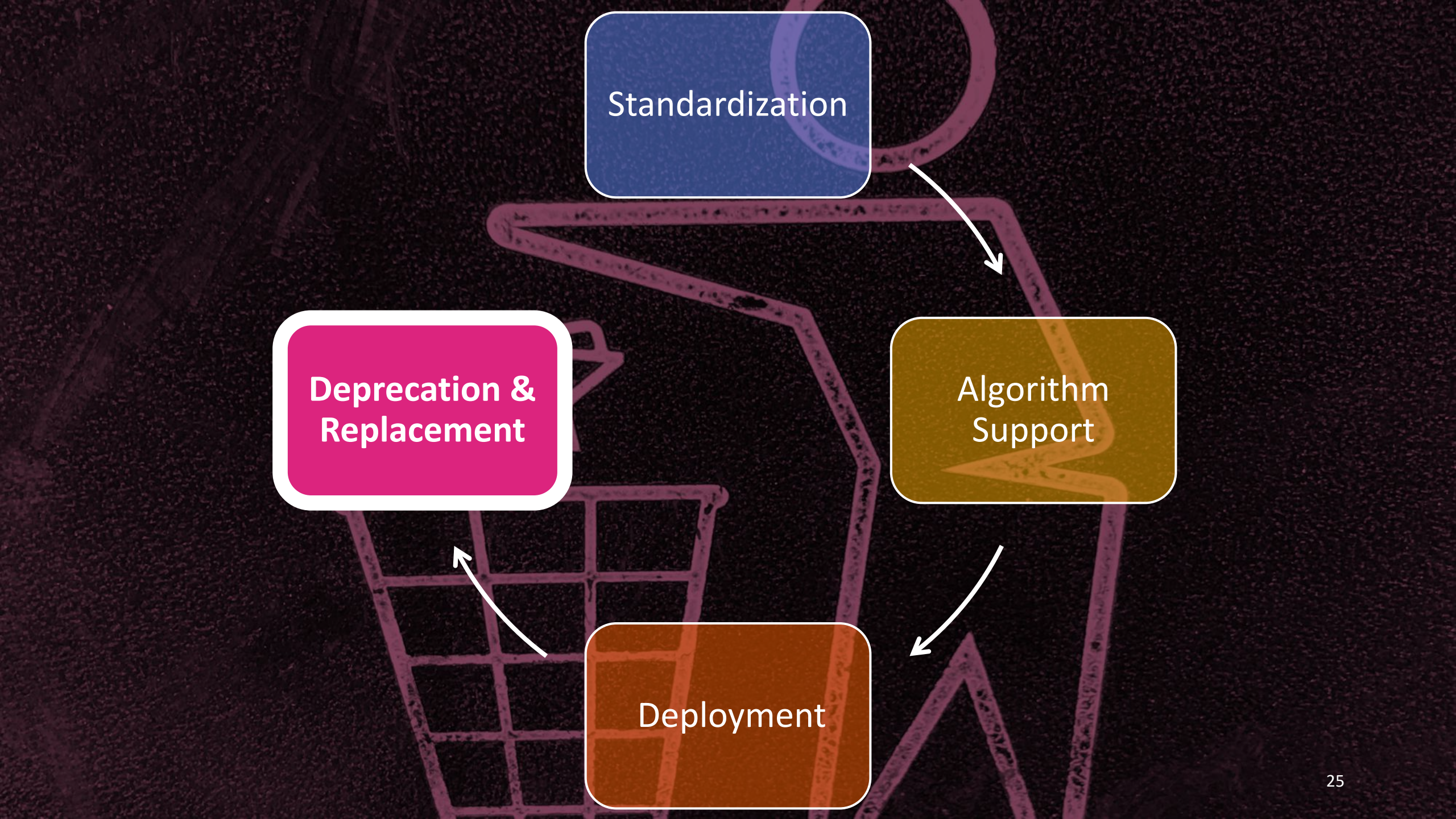


Algorithm Deployment at Resolvers

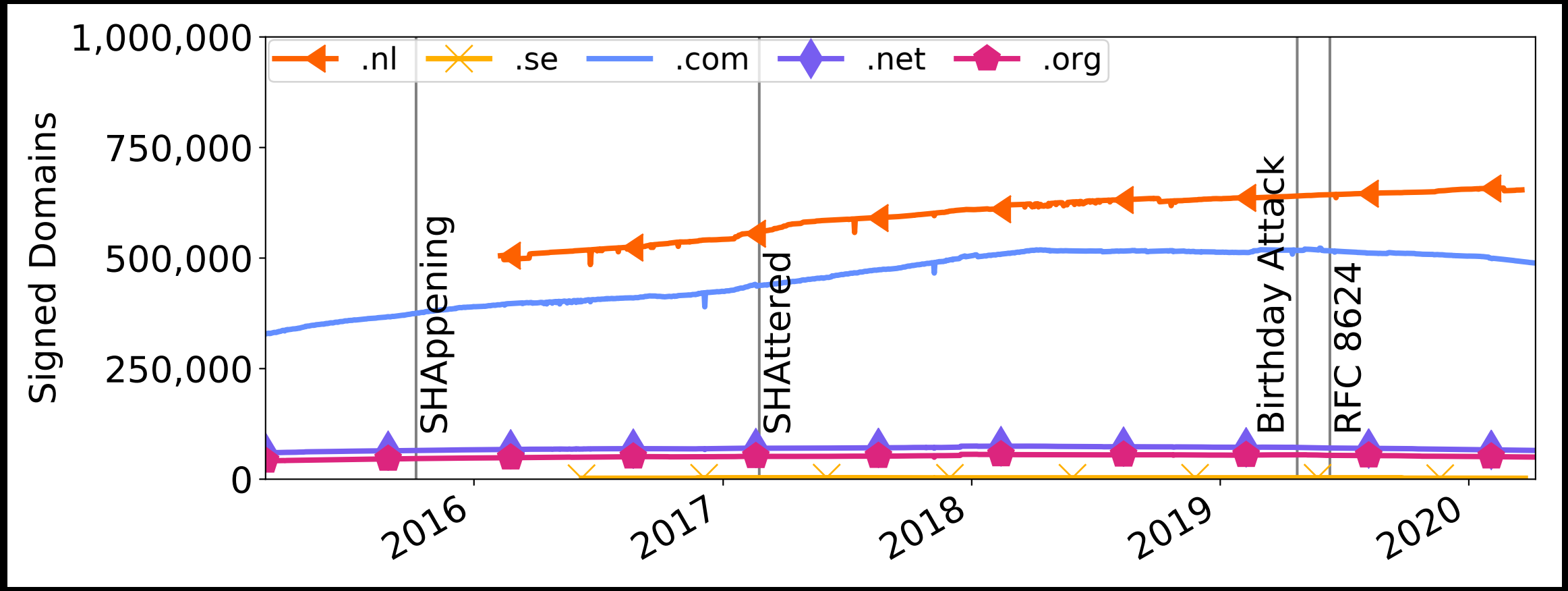


Algorithm Deployment at Resolvers



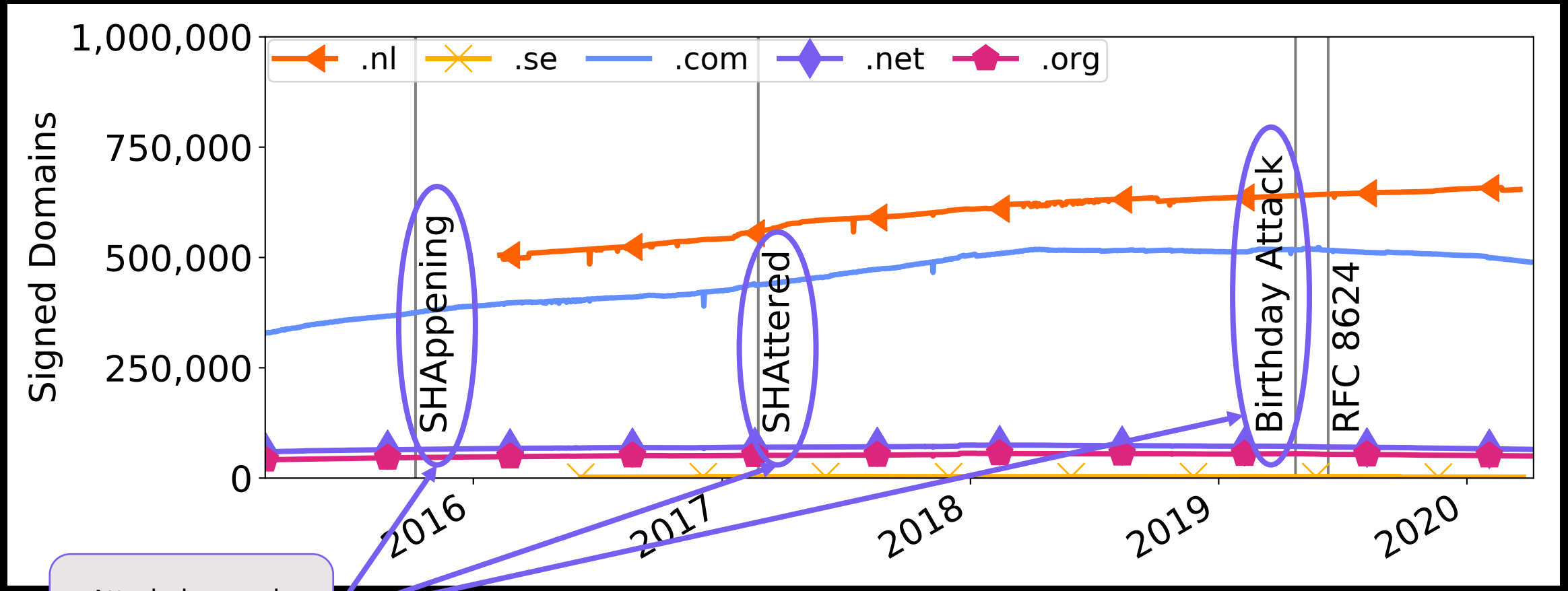

Standardization
Algorithm Support
Deployment
Deprecation & Replacement

Algorithm Deprecation at Domain Names

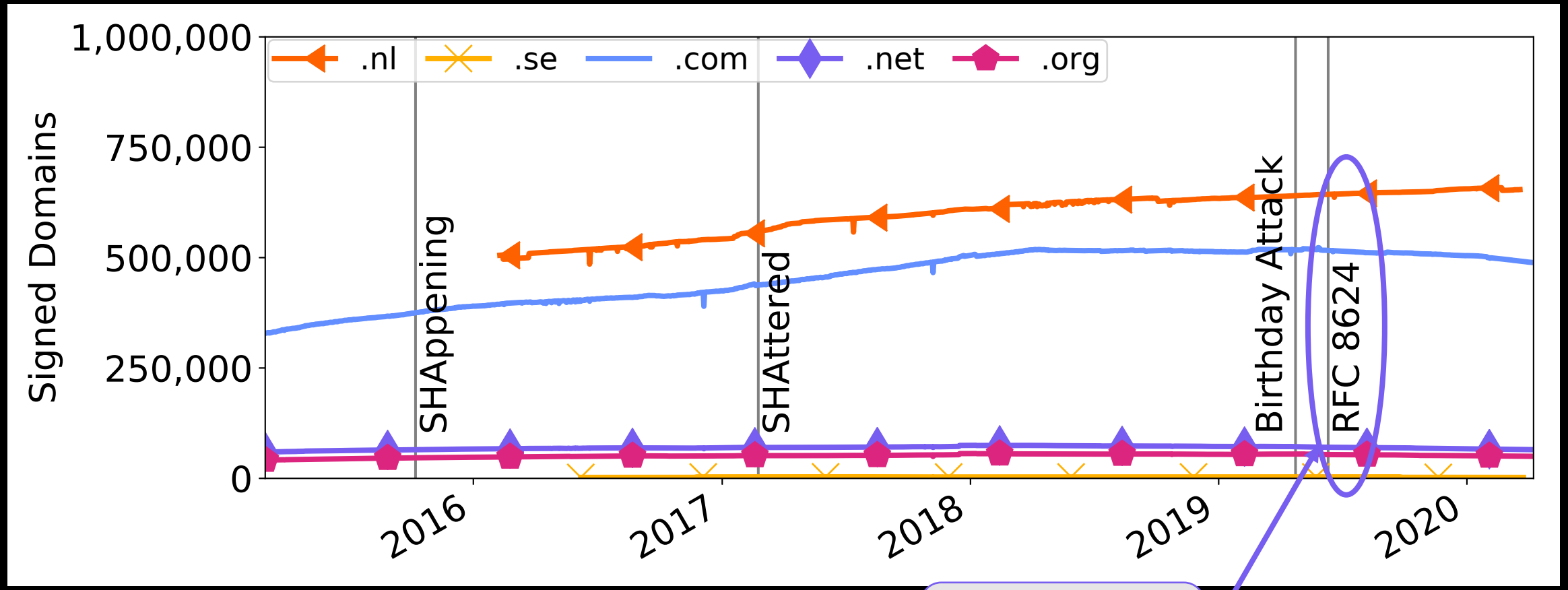


RSA-SHA1-NSEC3-SHA1

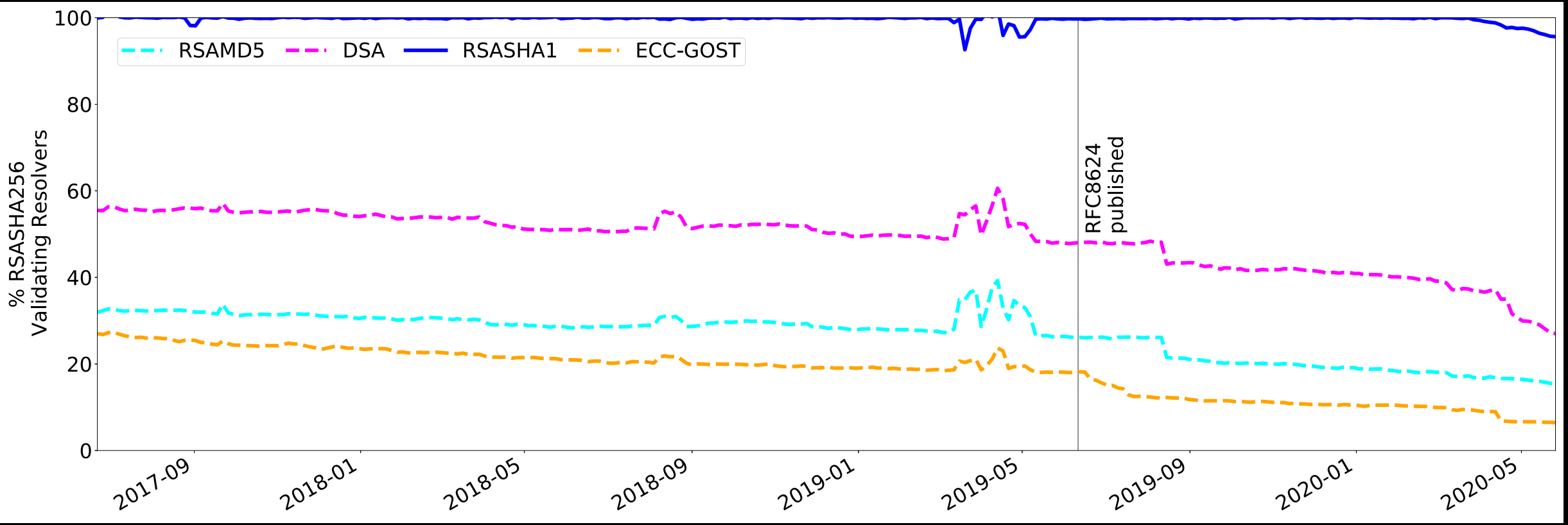
Algorithm Deprecation at Domain Names



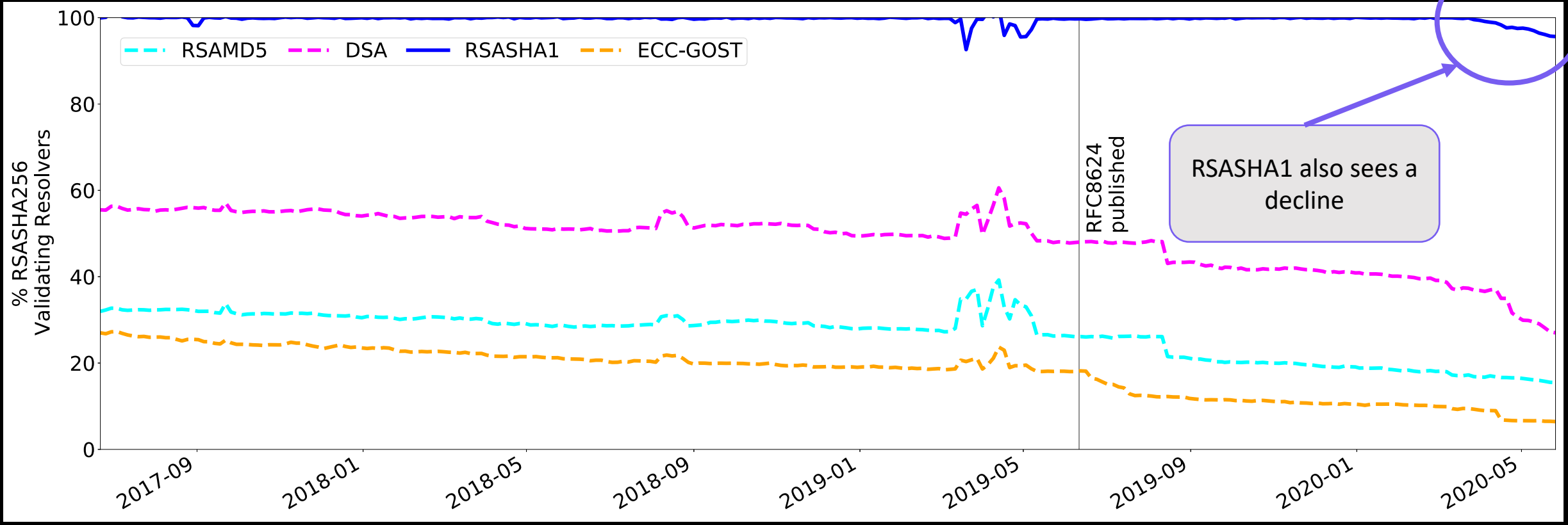
Algorithm Deprecation at Domain Names



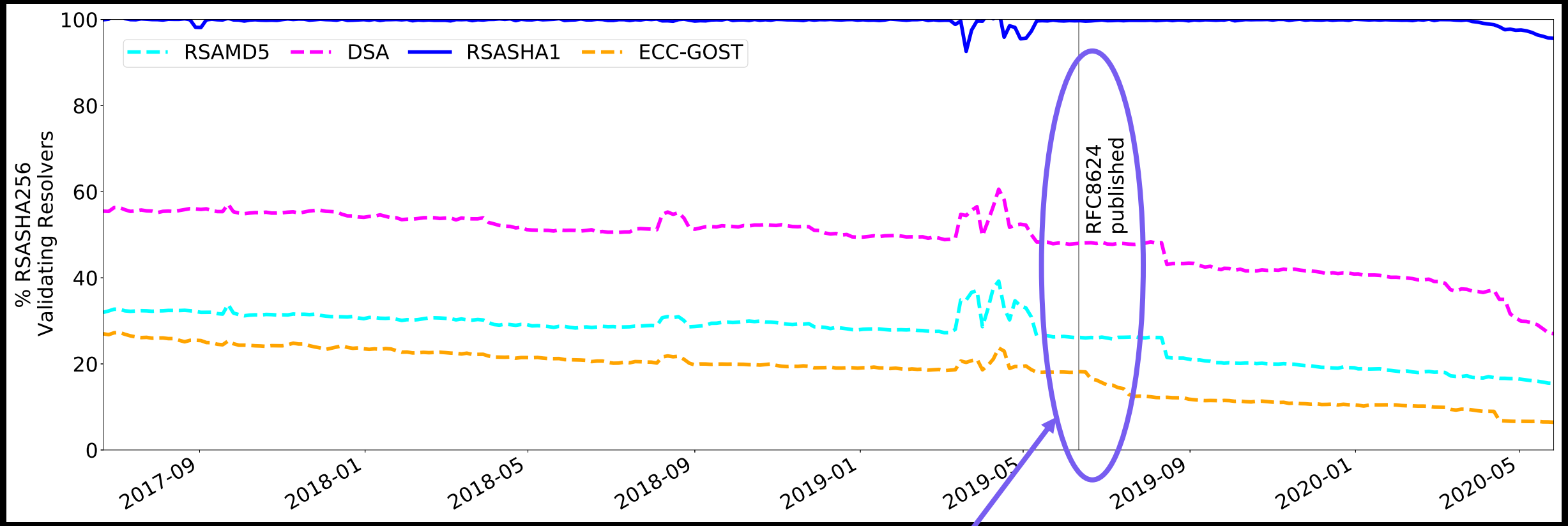
Algorithm Deprecation at Resolvers



Algorithm Deprecation at Resolvers



Algorithm Deprecation at Resolvers



Has DNSSEC achieved algorithm agility?

- Standardization, support and widespread deployment takes a decade
- DNSSEC is rarely the problem
- But lack of support in software and in the registration channel
- And the complexity of algorithm rollovers

Implications on the Transition to Quantum-Safe Algorithms

- Already transitioning to **current** algorithms takes a lot of time
  - and the Root has not rolled its algorithm yet
- Assessing quantum-safe algorithms as early as possible
- Take barriers into account

Implications on the Transition to Quantum-Safe Algorithms

- Already transitioning to **current** algorithms takes a lot of time
  - and the Root has not rolled its algorithm yet
- Assessing quantum-safe algorithms as early as possible
- Take barriers into account

Questions, suggestions, comments?

Contact
Moritz Müller | moritz.muller@sidn.nl | sidnlabs.nl