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]

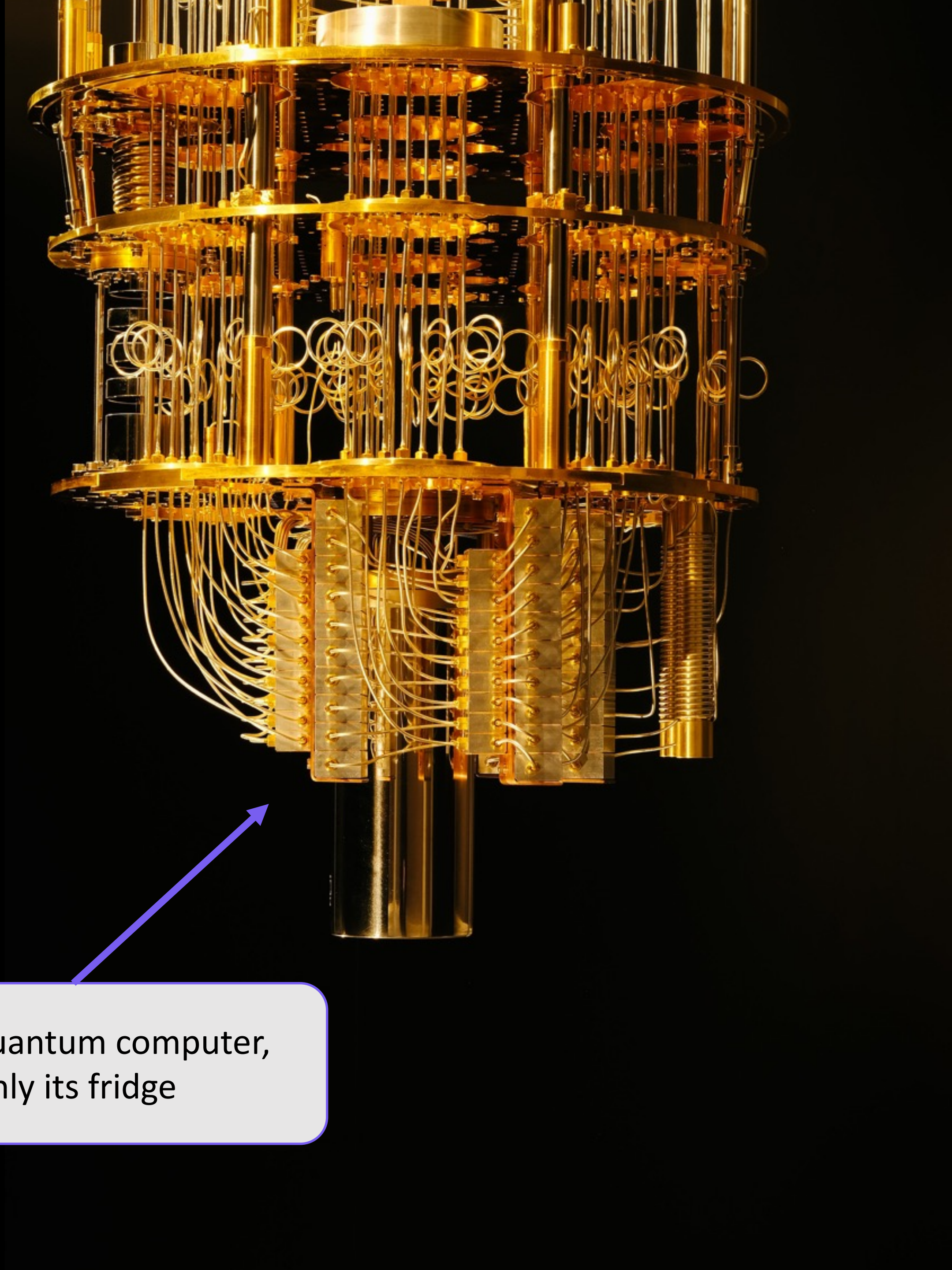
[1]NLnet Labs, [2]Virginia Tech, [3]SIDN Labs, [4]University of Twente

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

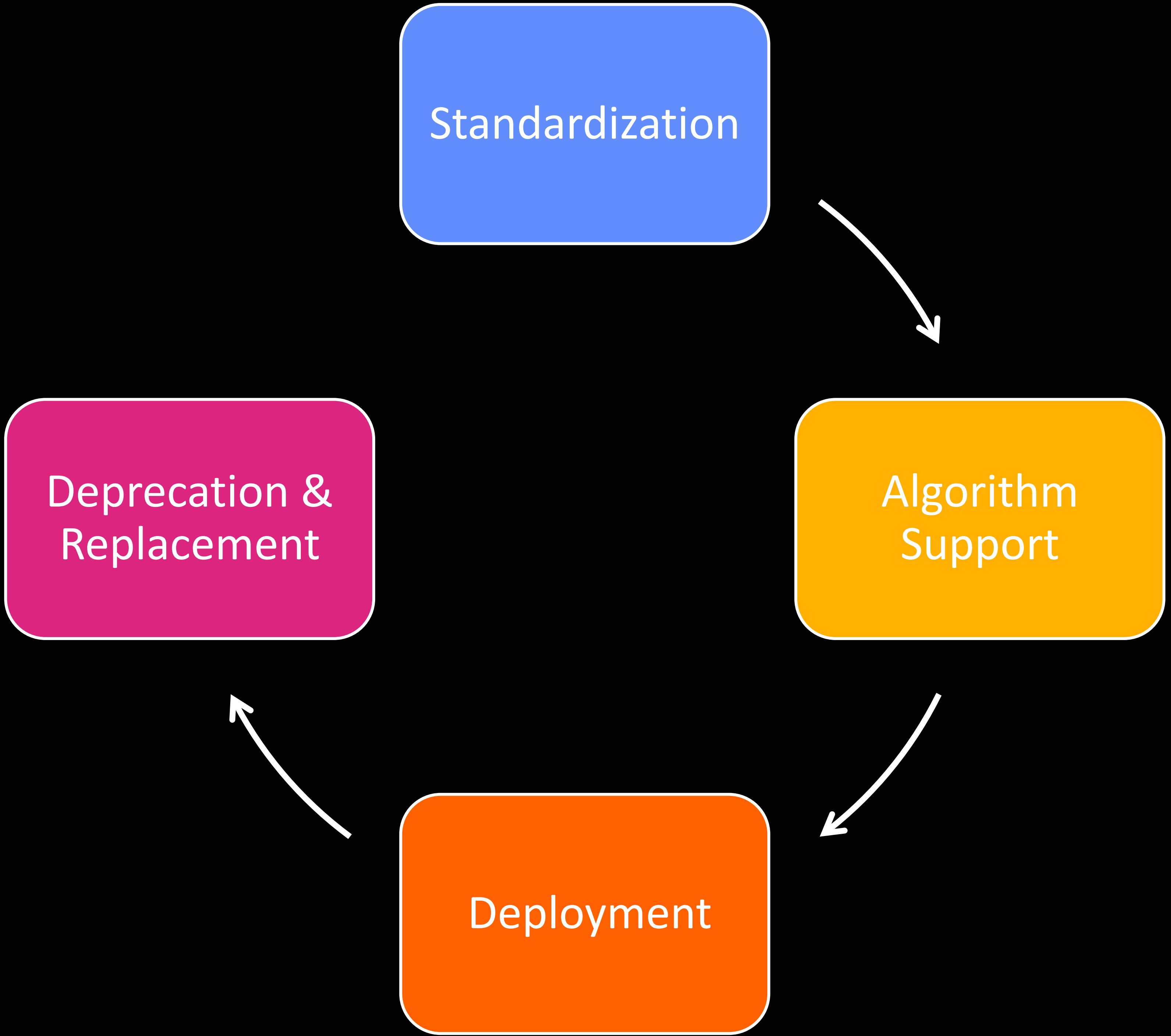
Introduction

- 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

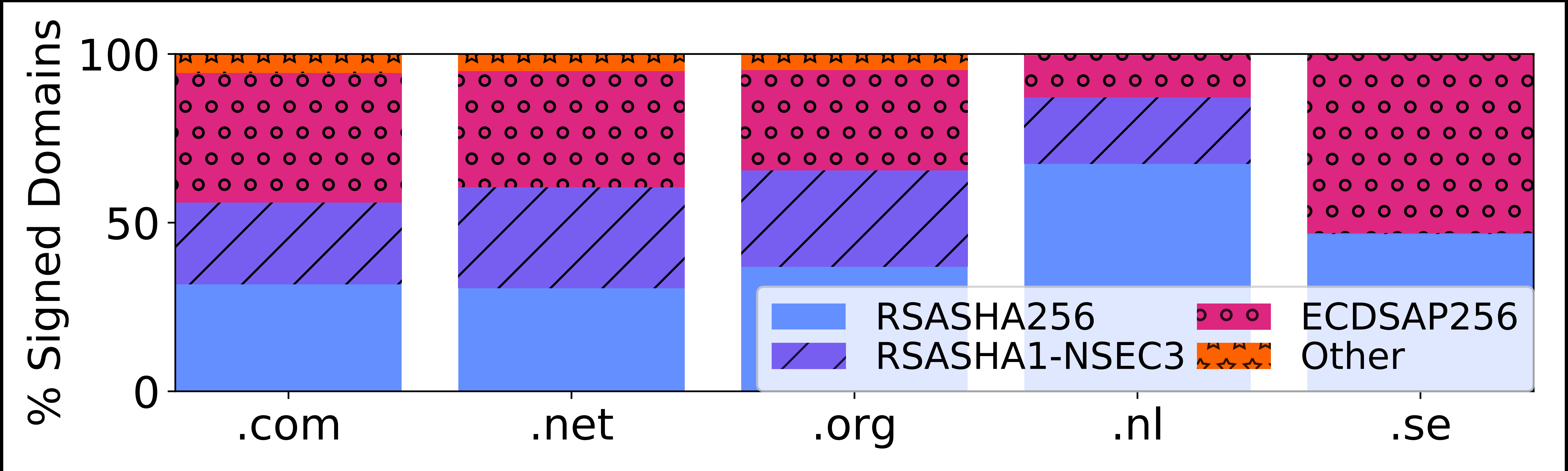
Algorithm Lifecycle

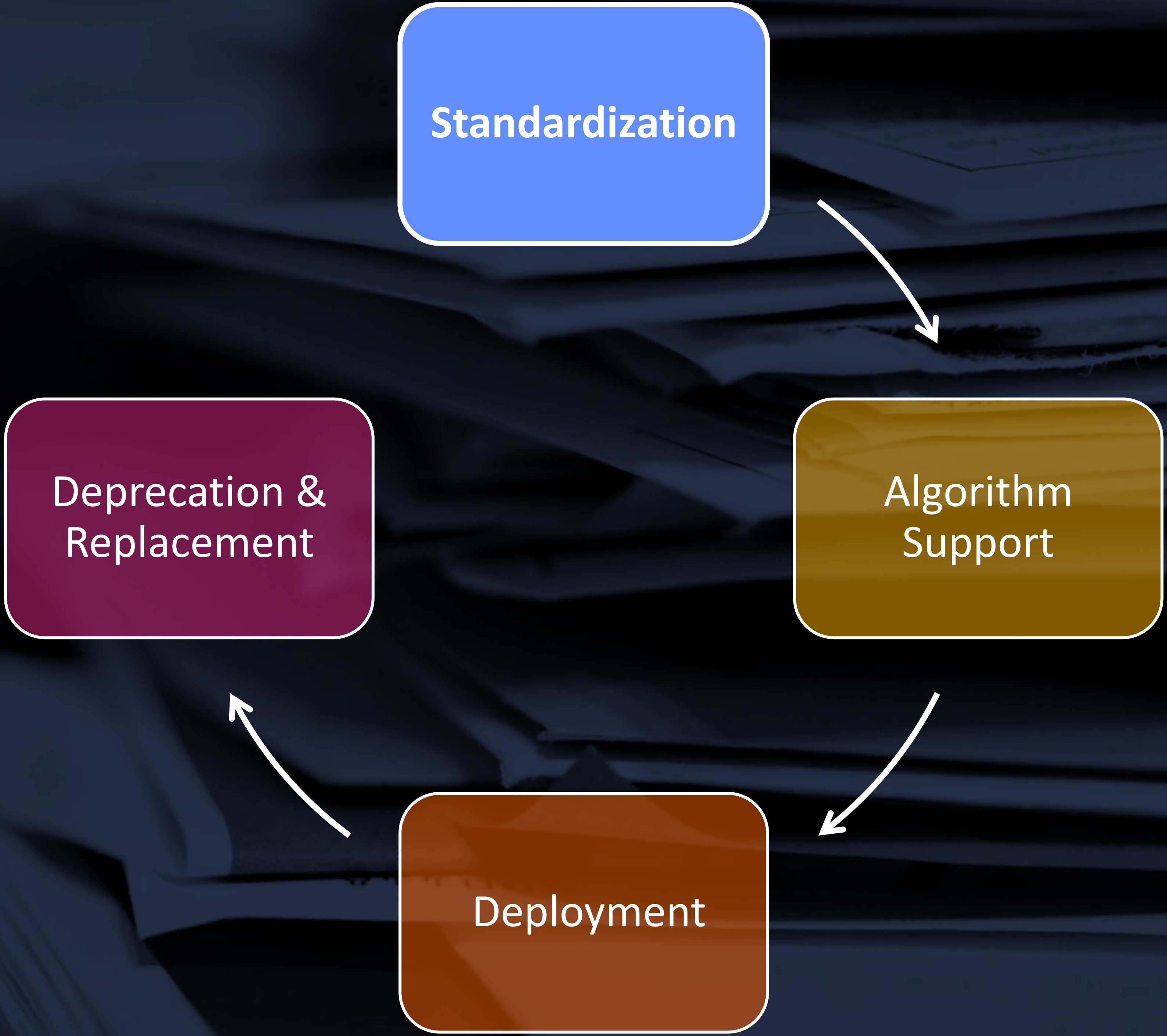


Analyzed Algorithms

- **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





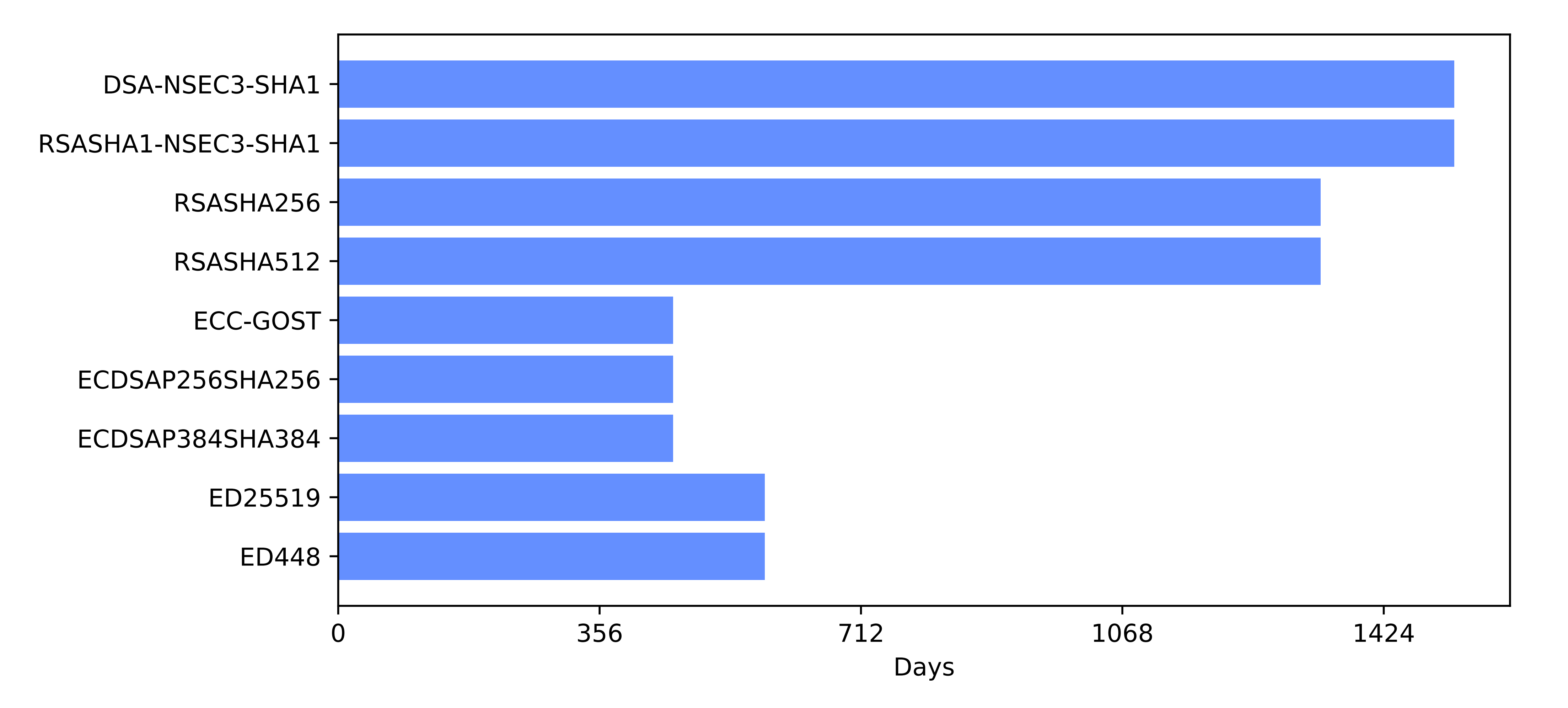
Standardization

Algorithm Support

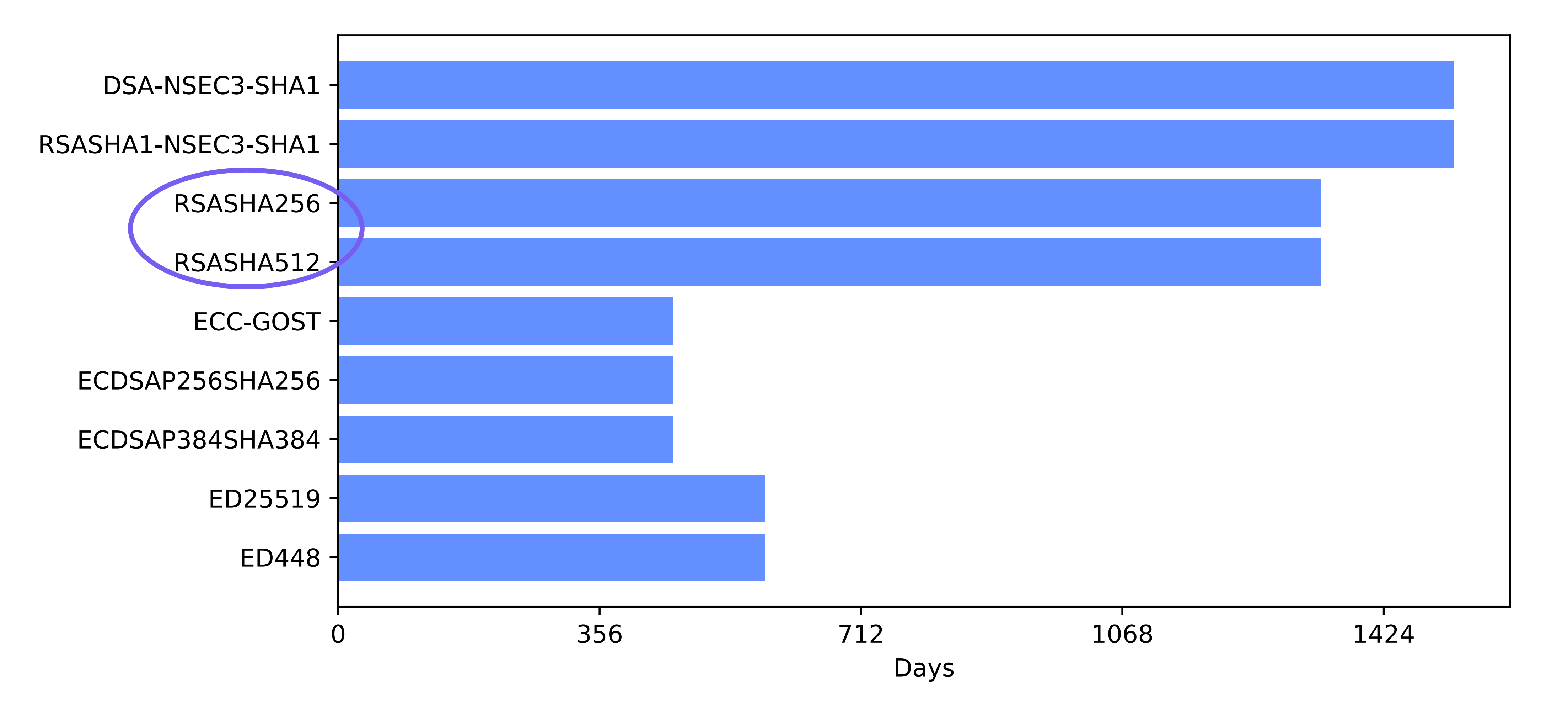
Deployment

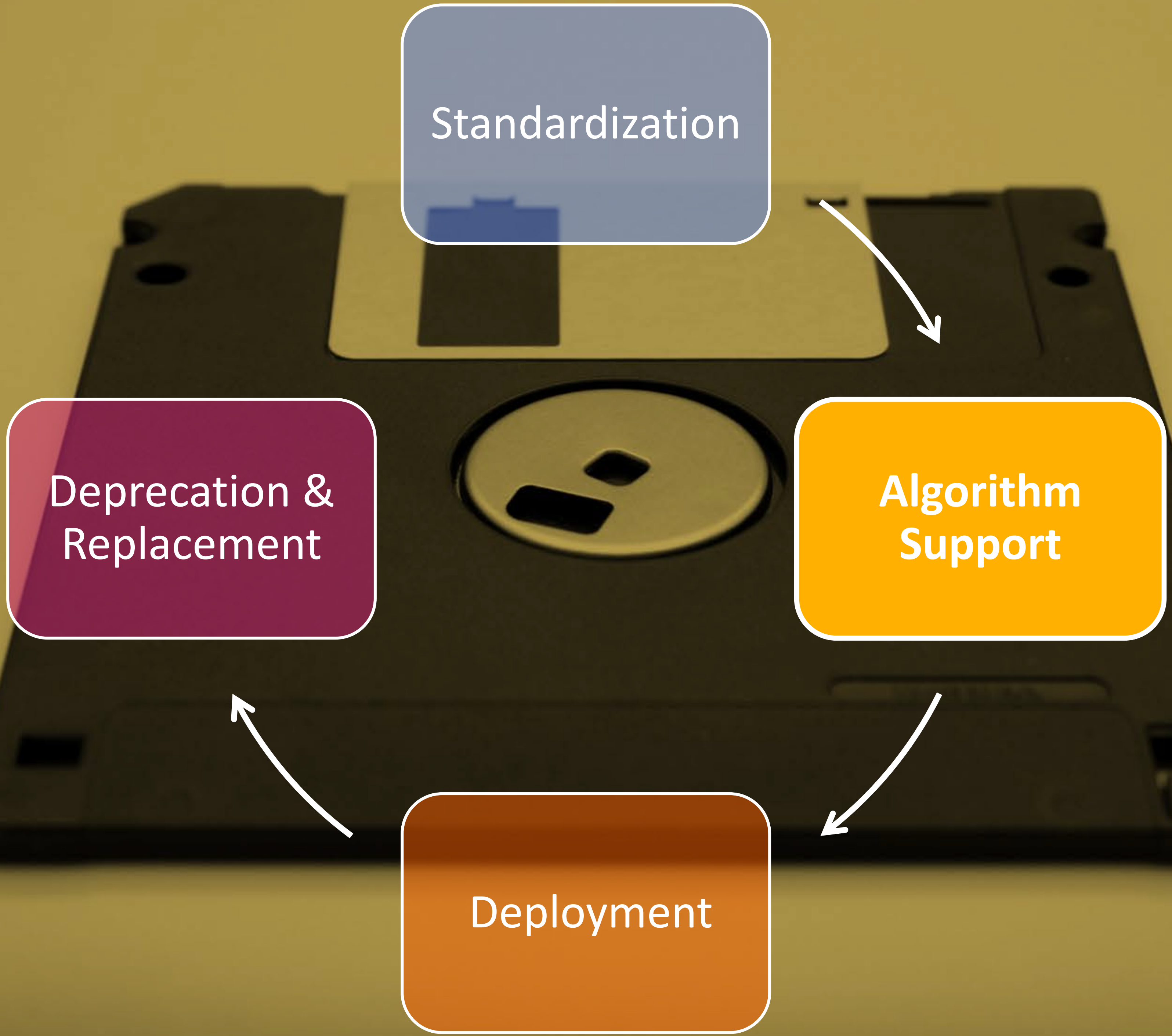
Deprecation & Replacement

Time until Standardization



Time until Standardization





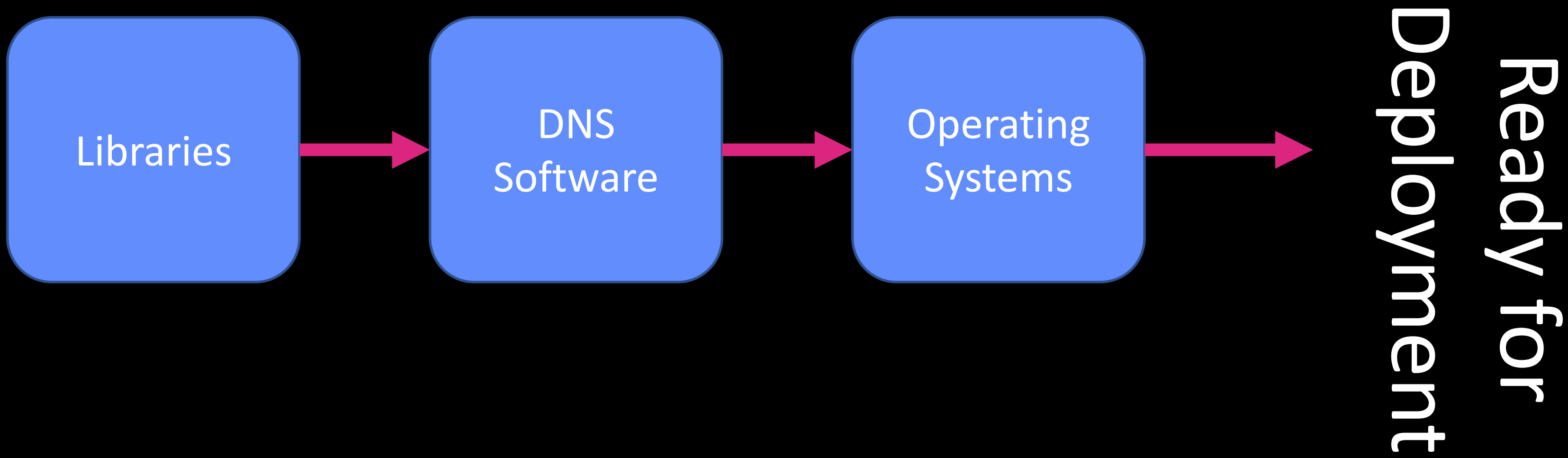
Standardization

Algorithm Support

Deployment

Deprecation & Replacement

Path to Full Support



Libraries

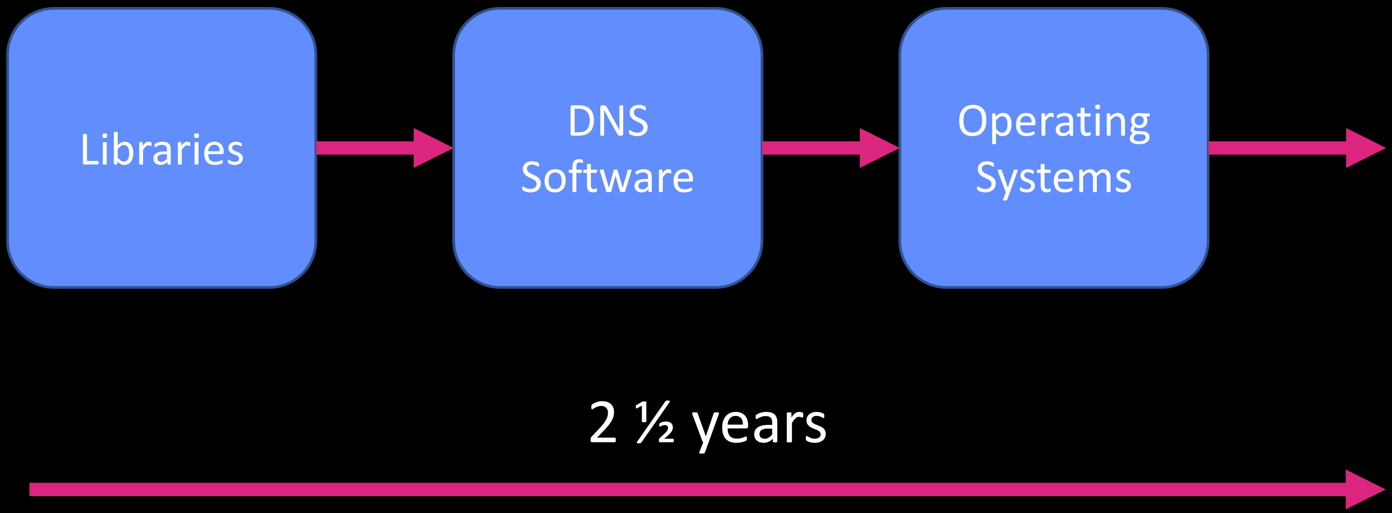
DNS Software

Operating Systems

Ready for Deployment

Photo by Josiah Farrow on Unsplash

Path to Full Support



Libraries

DNS Software

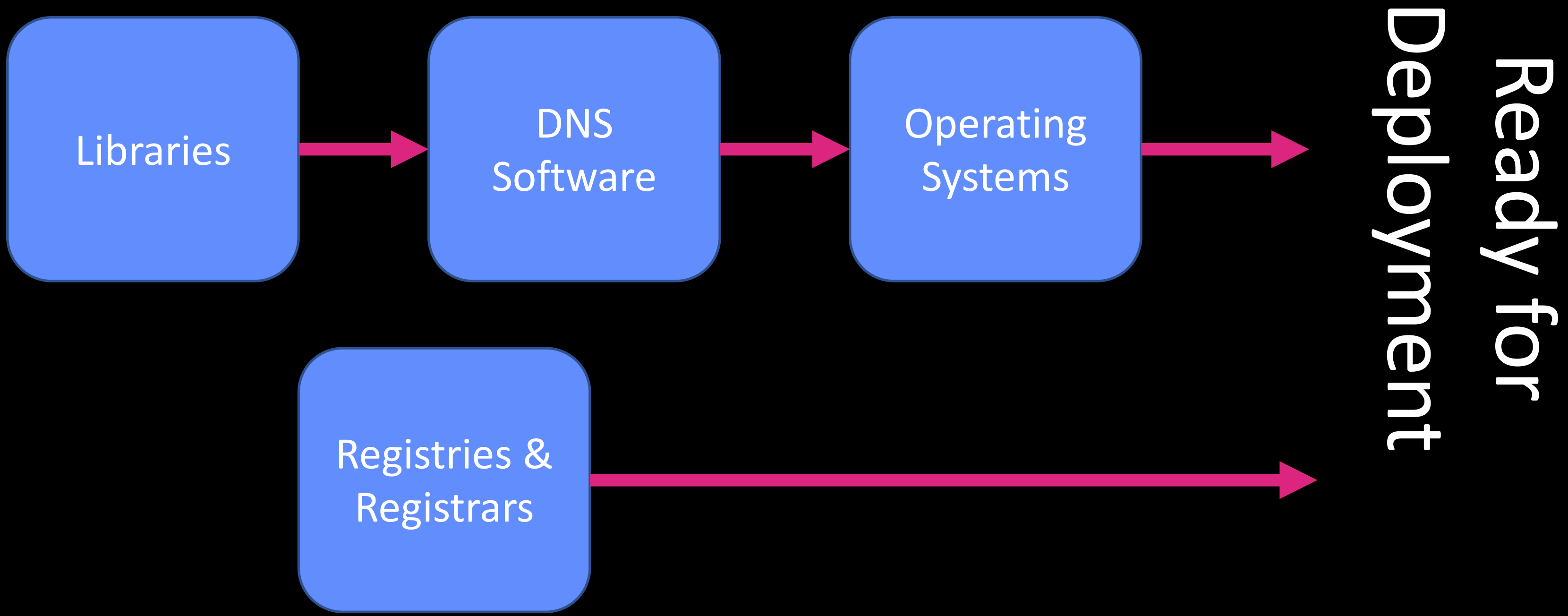
Operating Systems

2 ½ years

Ready for Deployment

ED25519: Ubuntu 18.04 & OpenSSL

Path to Full Support



Libraries

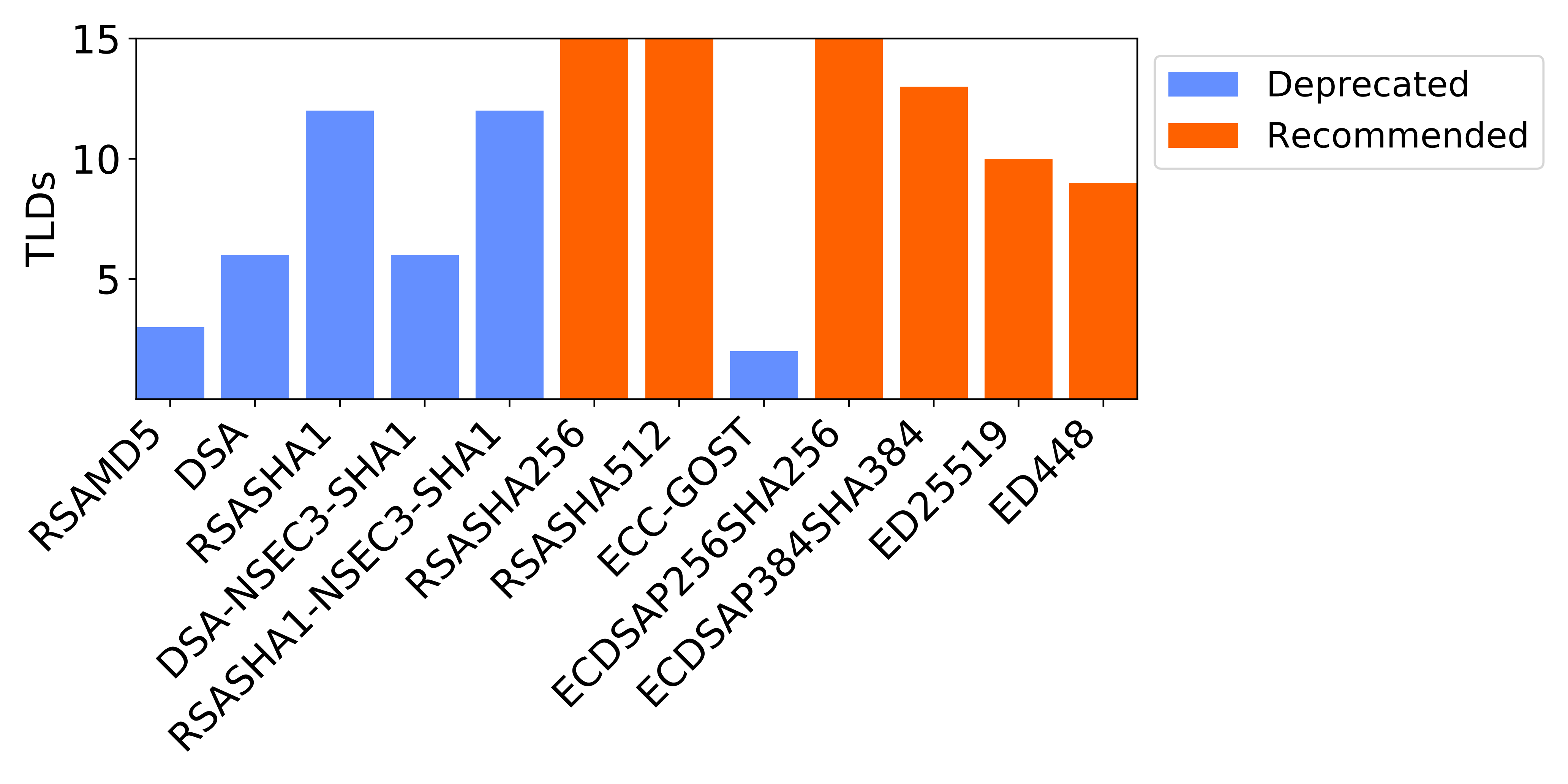
DNS Software

Operating Systems

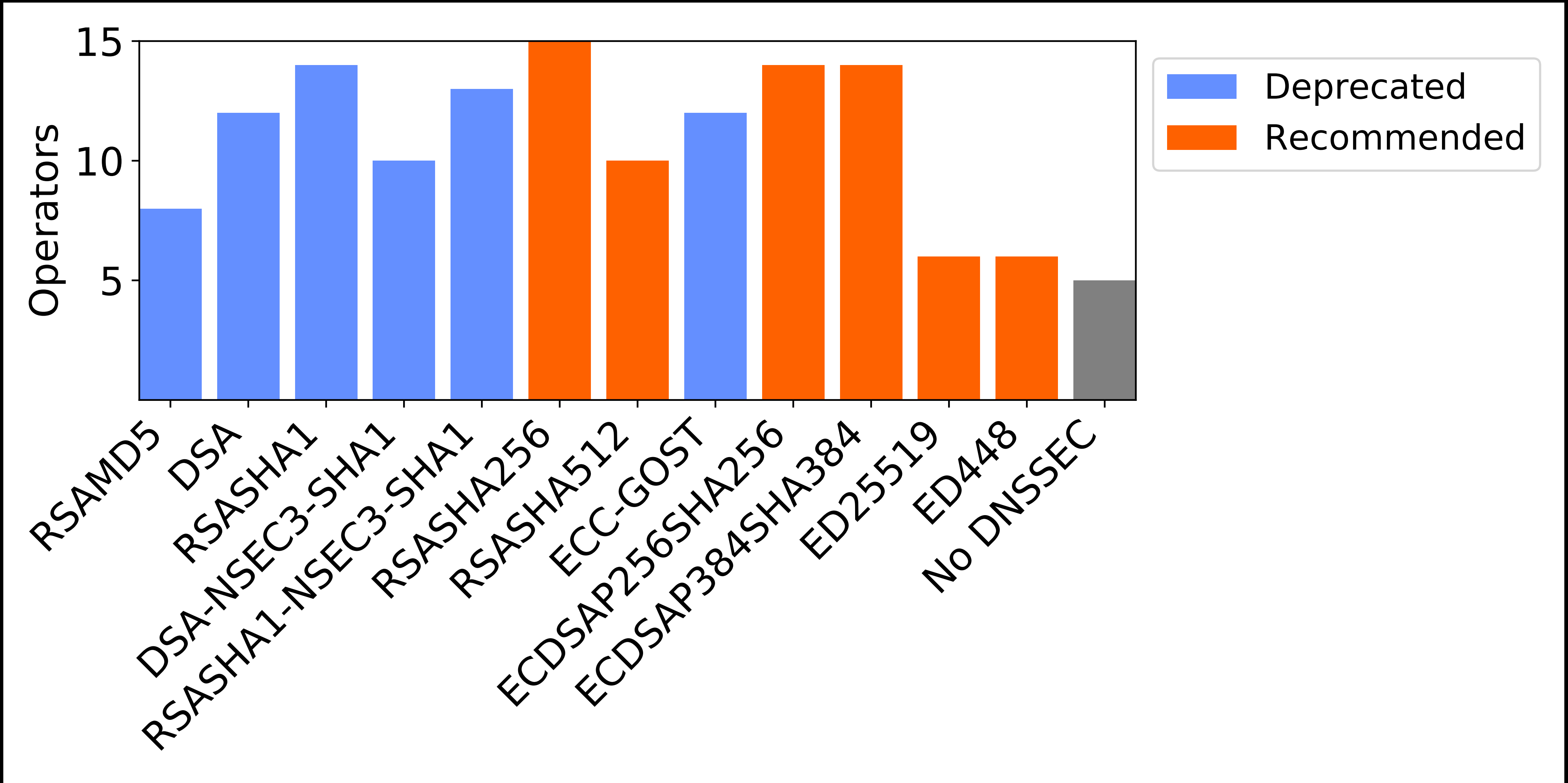
Registries & Registrars

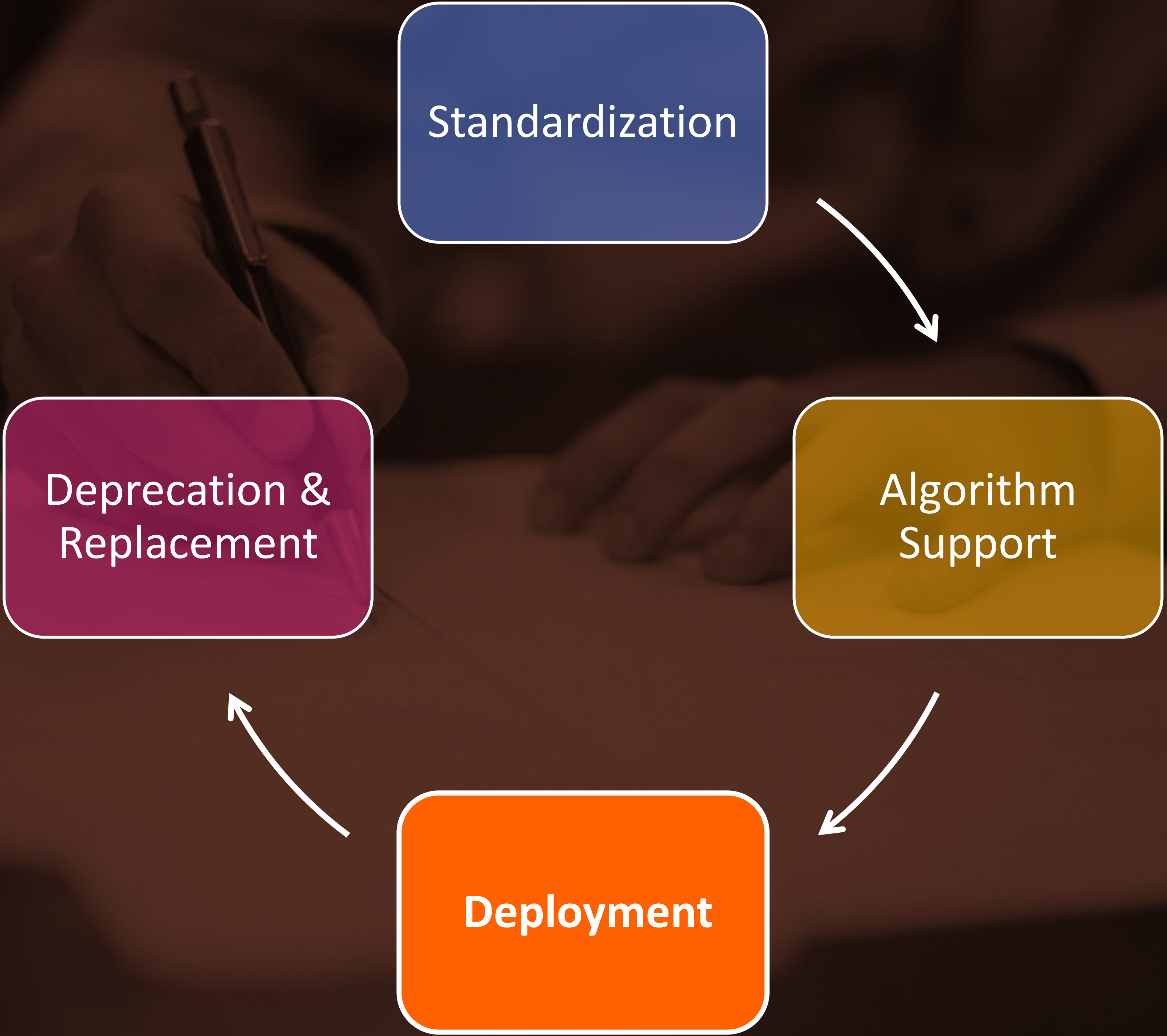
Ready for Deployment

Registry Support



Registrar Support





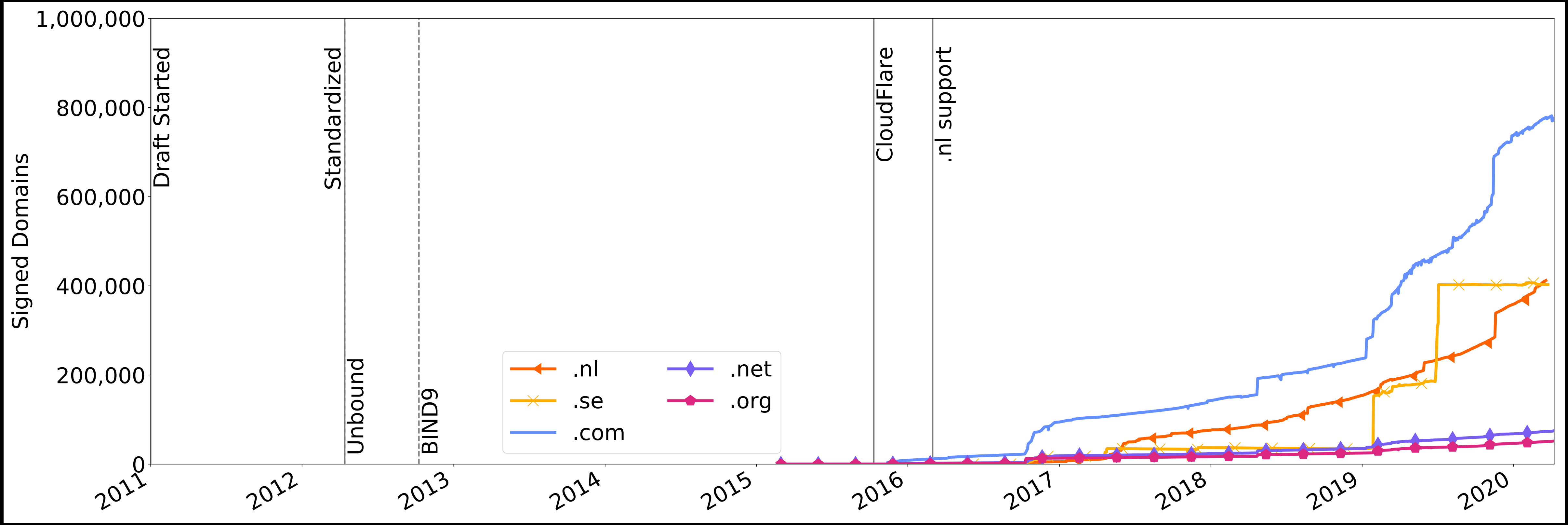
Standardization

Algorithm Support

Deployment

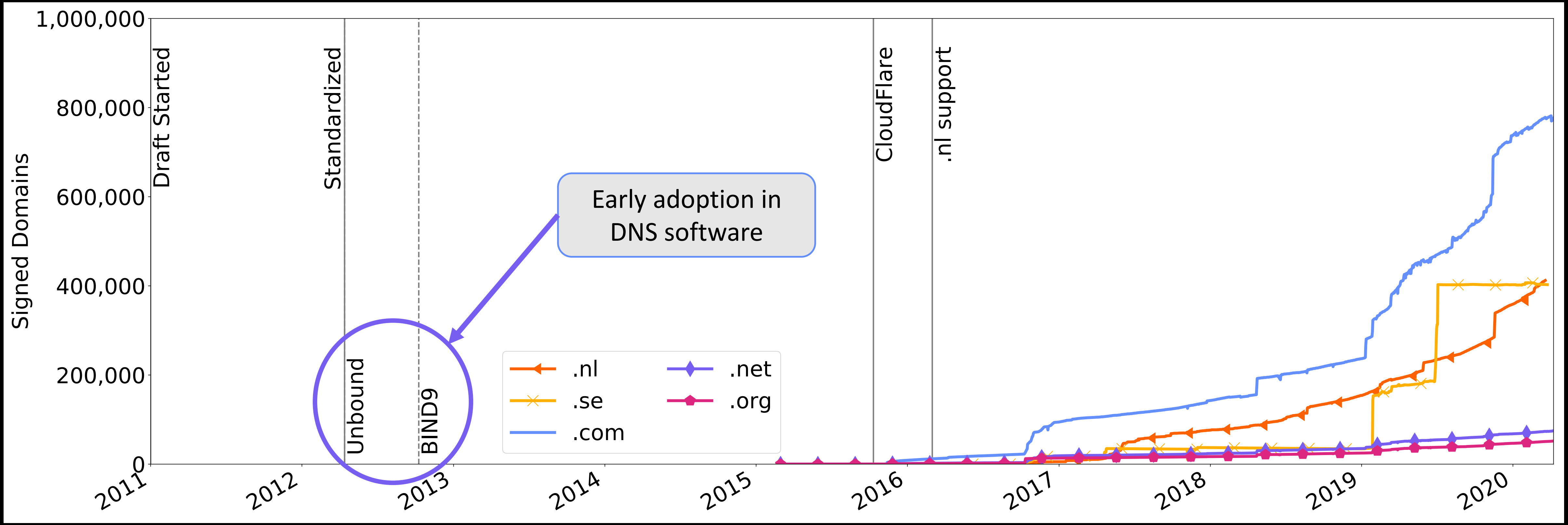
Deprecation & Replacement

Algorithm Deployment at Domain Names



ECDSA256

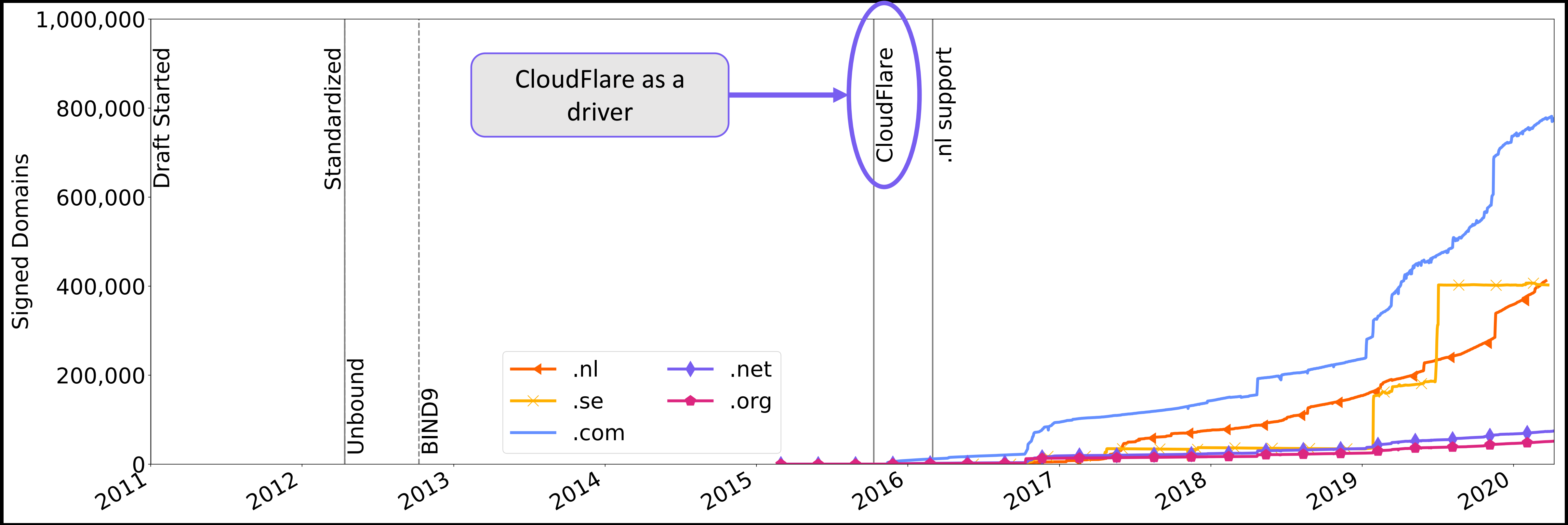
Algorithm Deployment at Domain Names



Early adoption in DNS software

ECDSA256

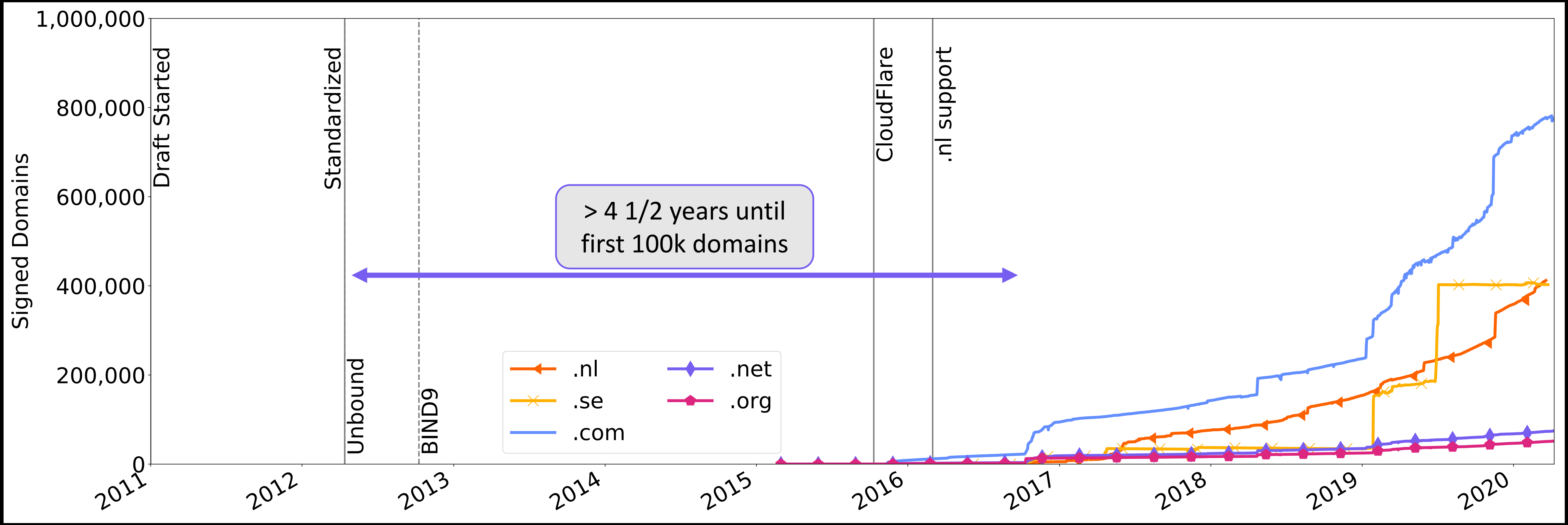
Algorithm Deployment at Domain Names



CloudFlare as a driver

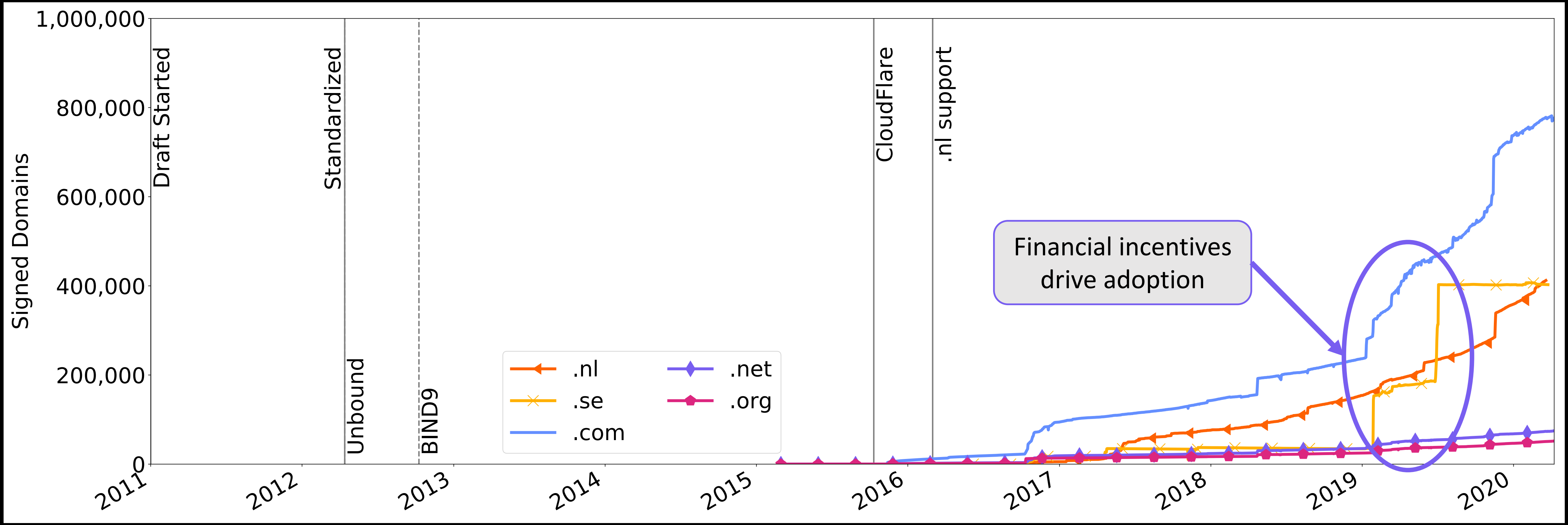
ECDSA256

Algorithm Deployment at Domain Names



ECDSA256

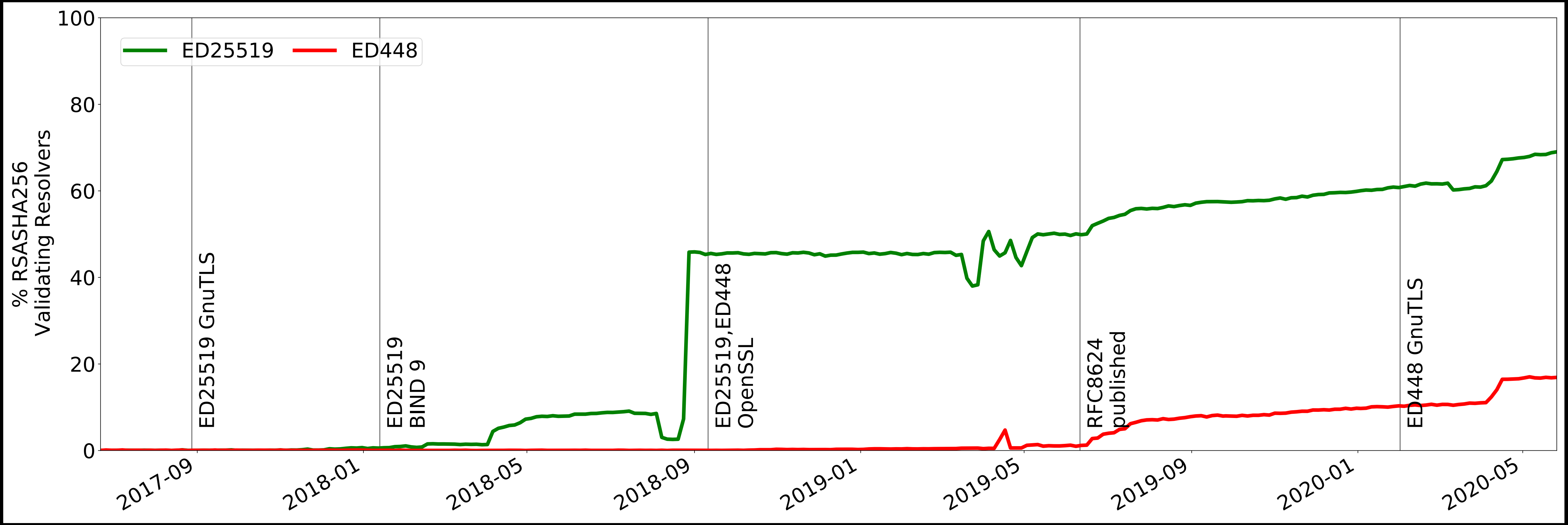
Algorithm Deployment at Domain Names



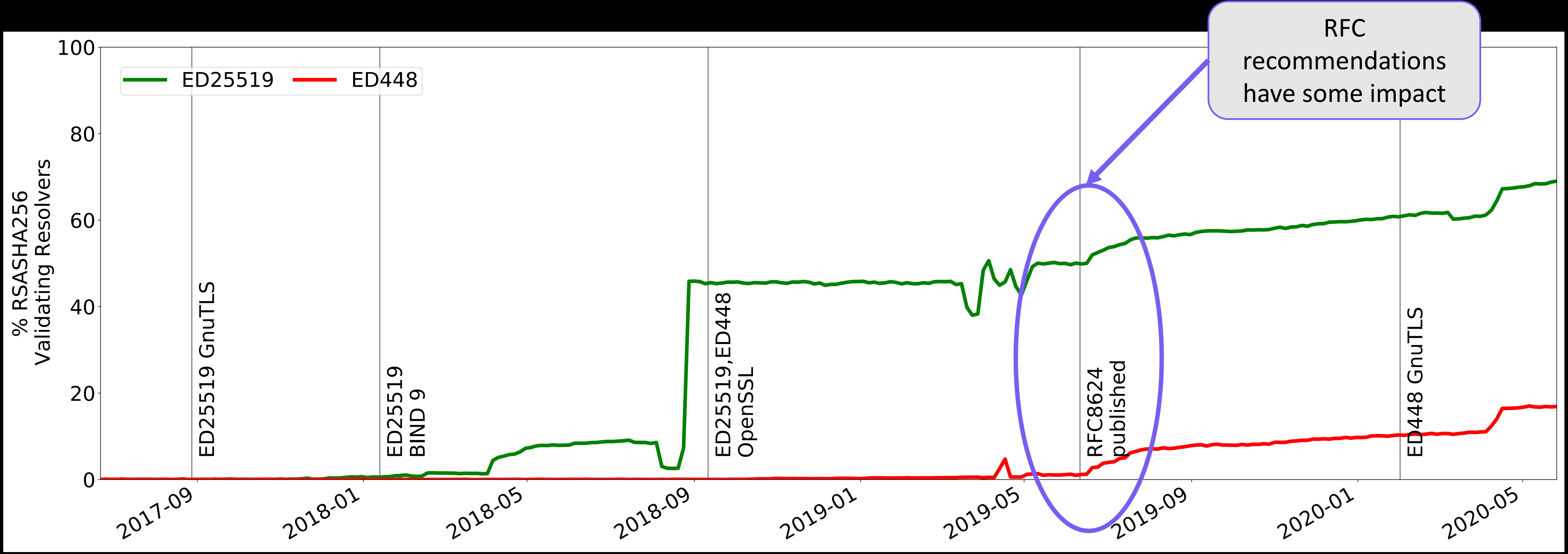
Financial incentives drive adoption

ECDSA256

Algorithm Deployment at Resolvers

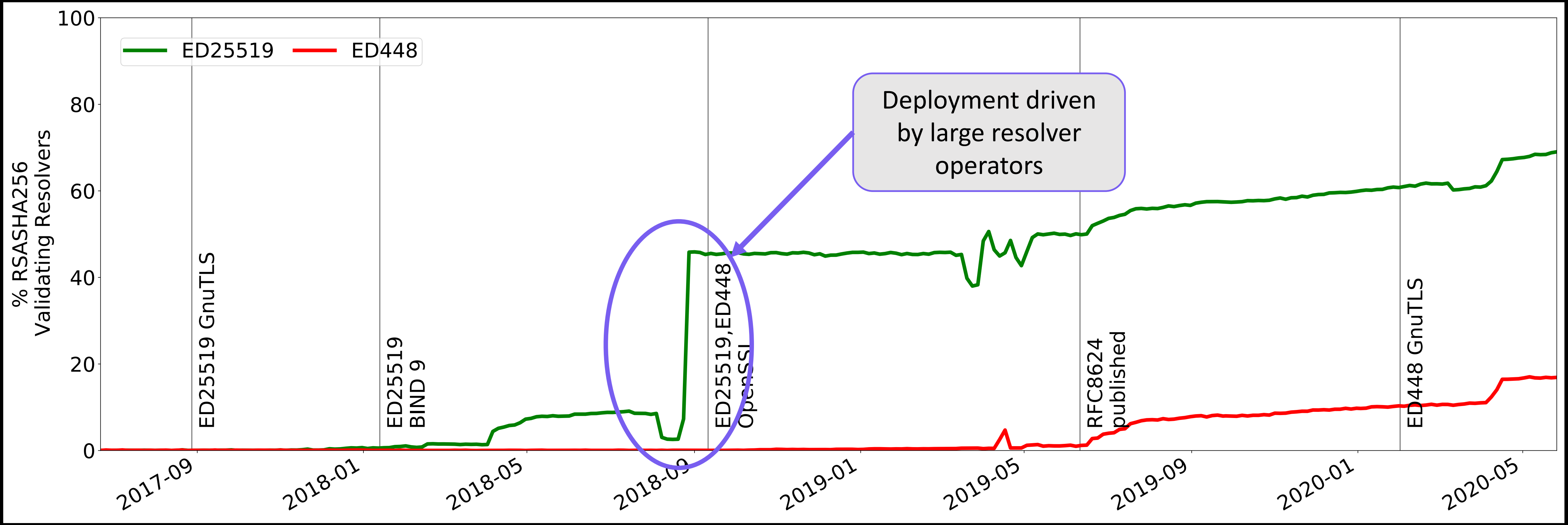


Algorithm Deployment at Resolvers

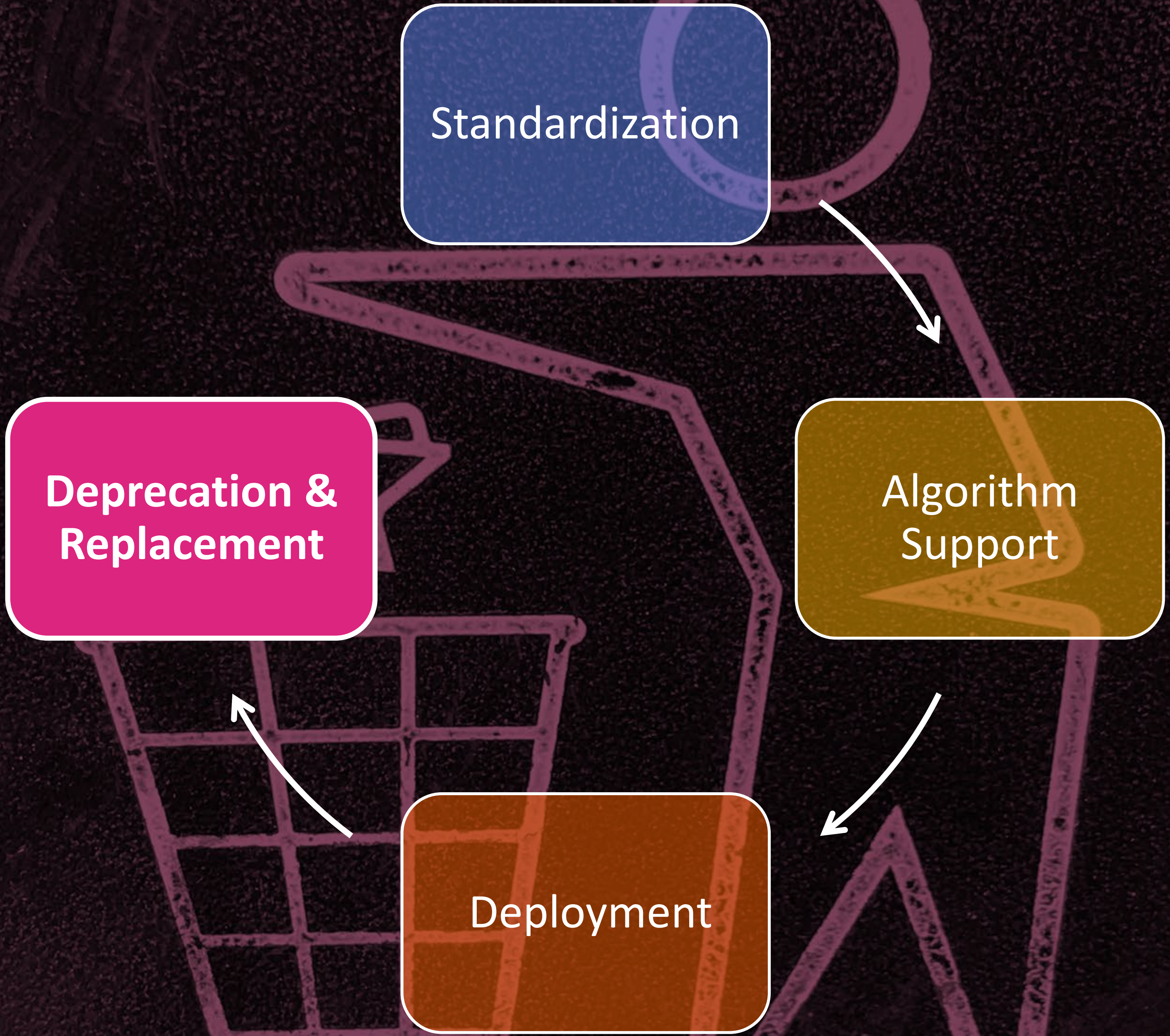


RFC recommendations have some impact

Algorithm Deployment at Resolvers



Deployment driven by large resolver operators



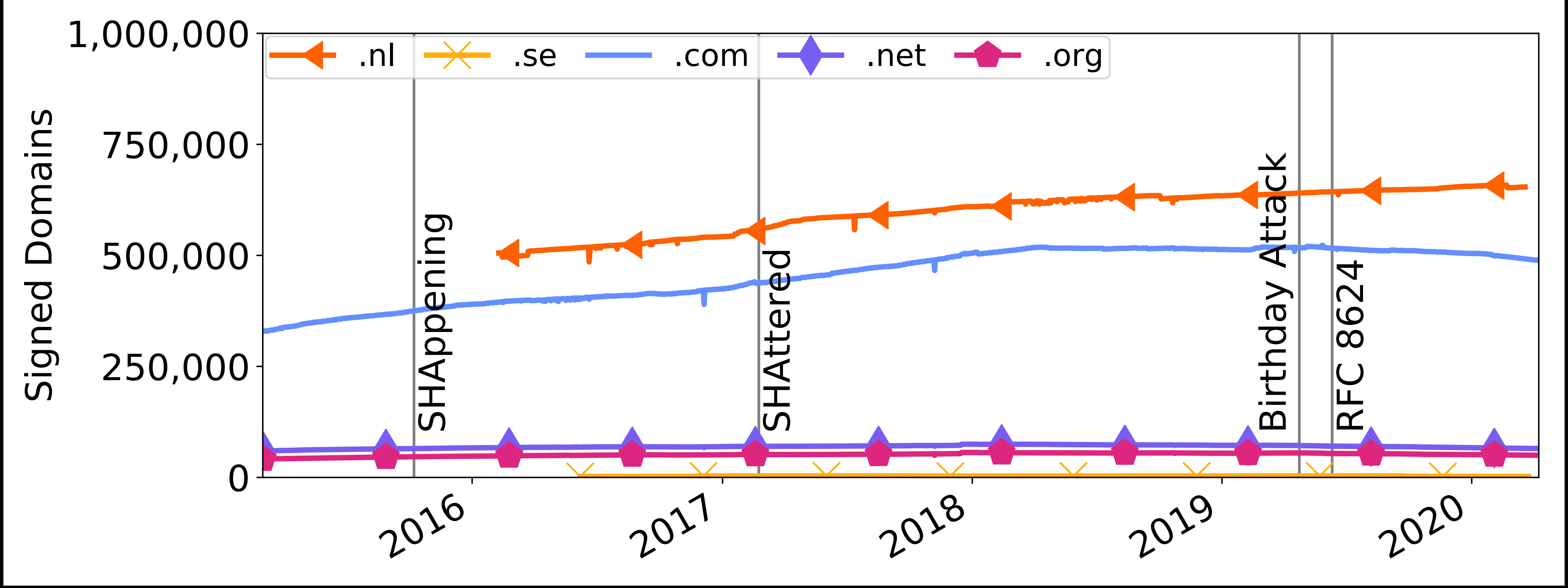
Standardization

Algorithm Support

Deployment

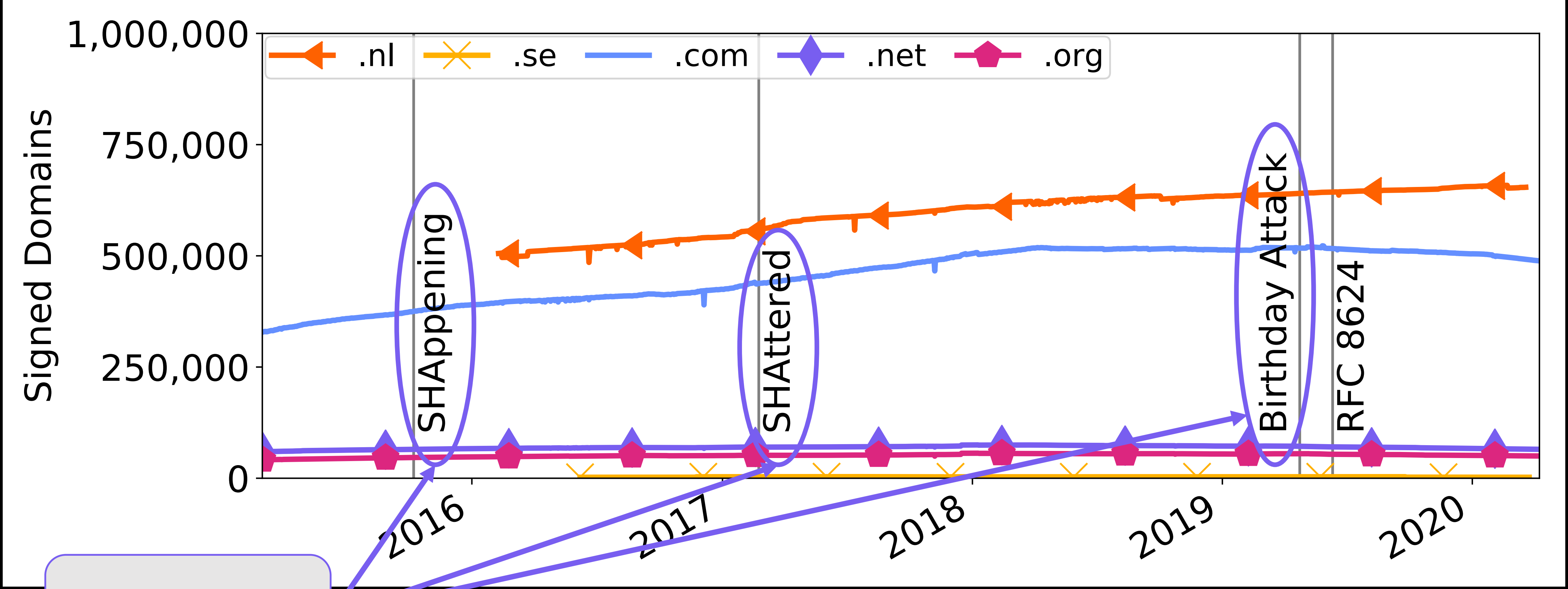
Deprecation & Replacement

Algorithm Deprecation at Domain Names



RSA-SHA1-NSEC3-SHA1

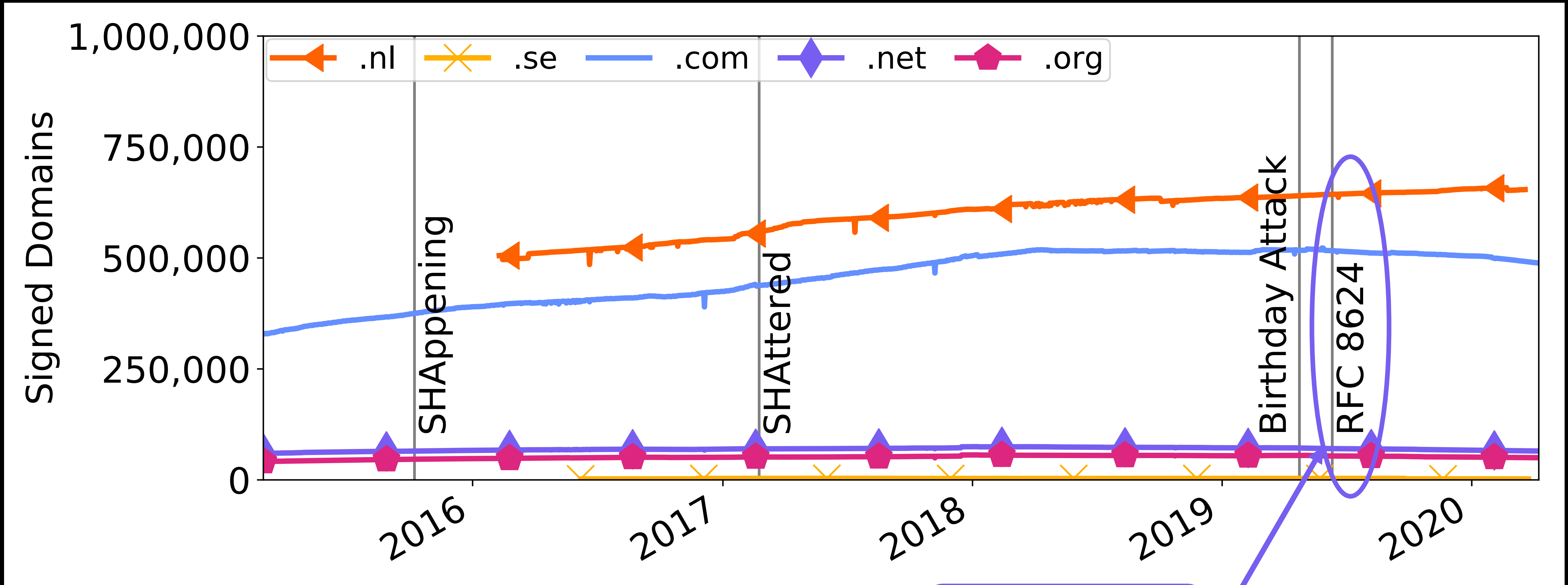
Algorithm Deprecation at Domain Names



Attacks have only minor impact

RSA-SHA1-NSEC3-SHA1

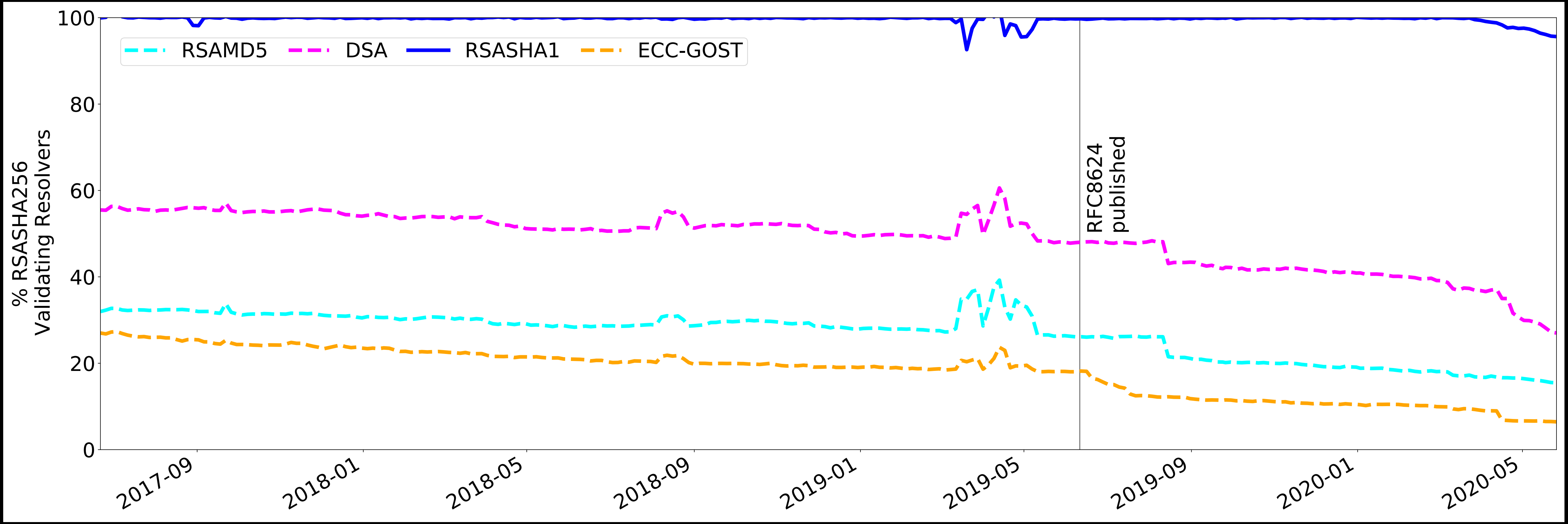
Algorithm Deprecation at Domain Names



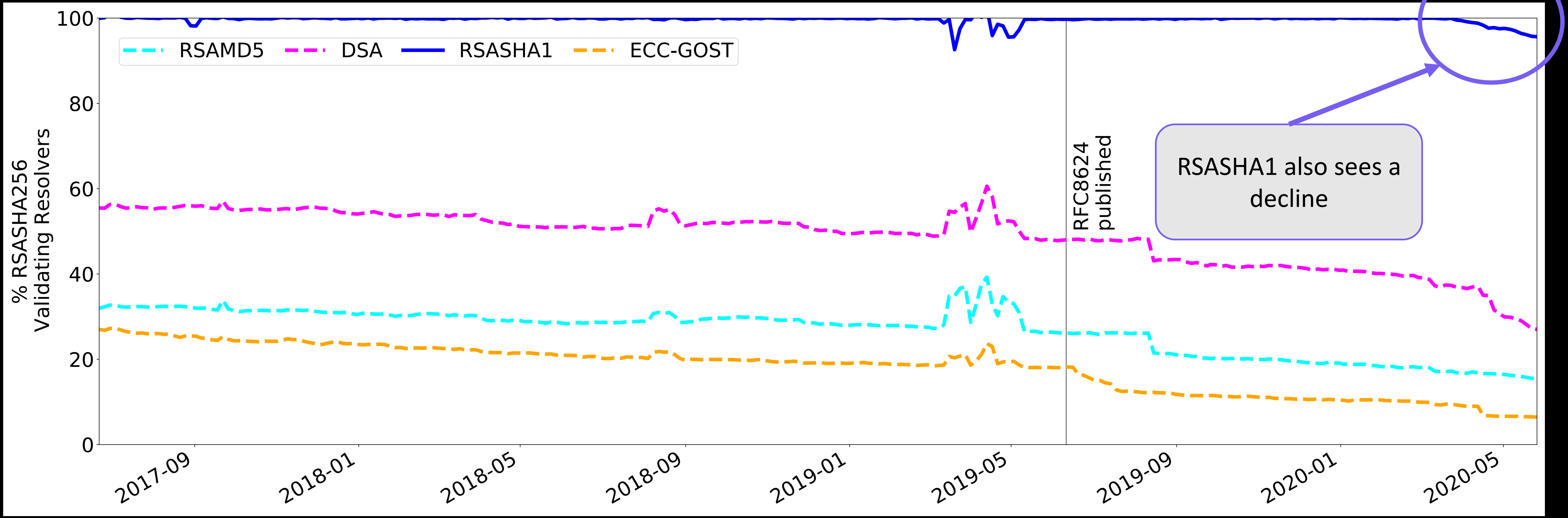
RSA-SHA1-NSEC3-SI

RFC recommendations have some impact

Algorithm Deprecation at Resolvers

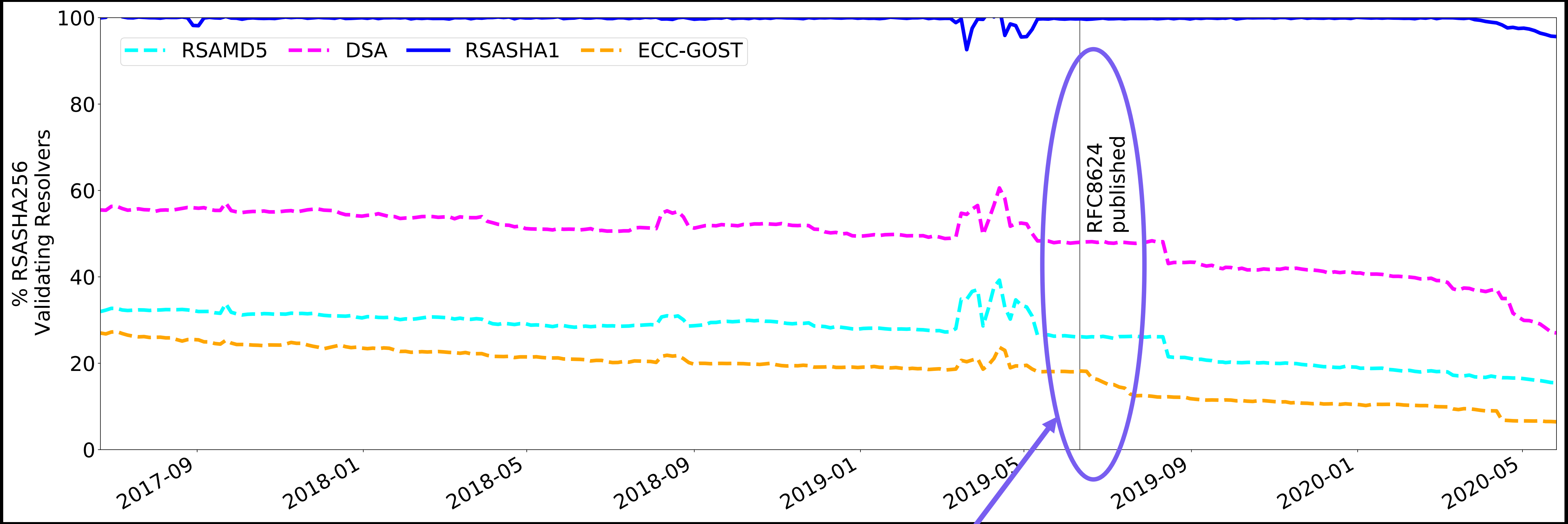


Algorithm Deprecation at Resolvers



RSASHA1 also sees a decline

Algorithm Deprecation at Resolvers



RFC recommendations speed up decline

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