Об использовании криптографических протоколов ГОСТ в протоколе DNSSec

Долматов Василий Вадимович

Заместитель генерального директора

«Криптоком»

криптоком

Принципиальные особенности DNS

- Древовидная структура с единым корнем
- Обязательность кэширования ответов
- Использование протокола UDP

криптоком

Проблемы DNS

- Уязвимость структуры к DoS атакам
- Cache poisoning
- Недостоверность источника

Модернизации DNS

- T-SIG
  - Криптозащита транспорта
- DNSSec
  - Криптозащита содержания ответов

Результаты модернизации DNS (DNSSec)

- Противостоит части атак на DNS (cache poisoning, modified data)
- Создает целый ряд новых проблем (увеличение нагрузки на серверы DNS, проблемы при key rollover, etc.)
- …
- Происходит поэтапное внедрение (07.2010 — signed root)

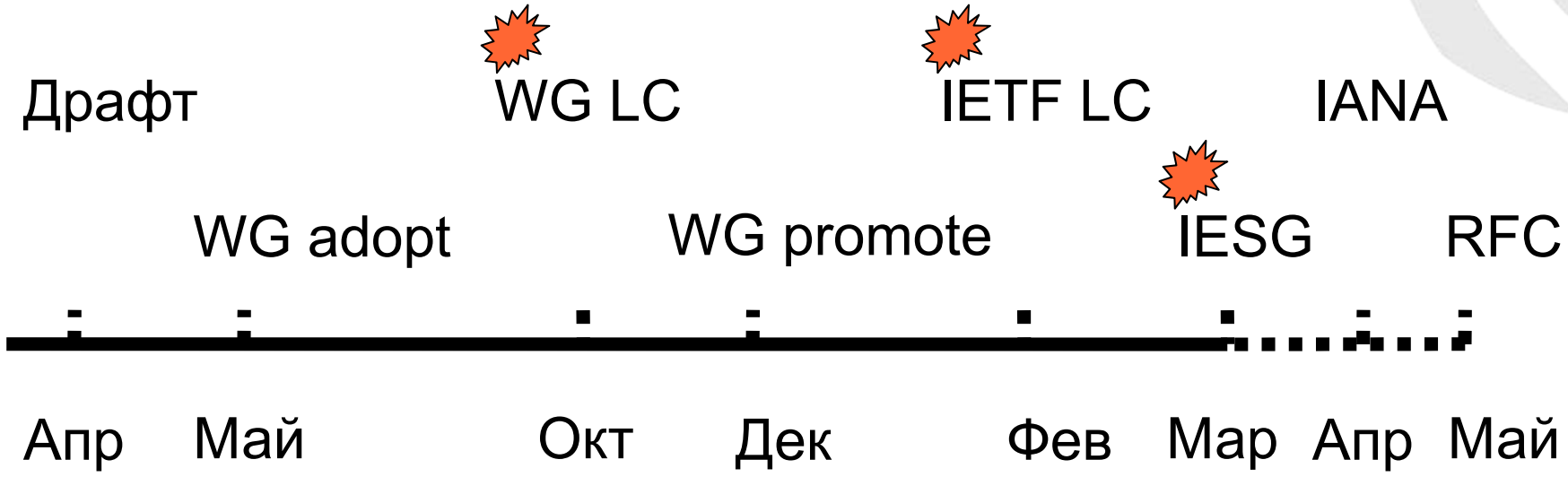
Криптографические протоколы в DNSSec

- Гибкая структура протоколов

Номер протокола	Код протокола
3	DSA/SHA1
4	...
5	RSA/SHA1
6	DSA-NSEC3-SHA1
7	RSASHA1-NSEC3-SHA1
8	RSA/SHA-256
9	...
10	RSA/SHA-512

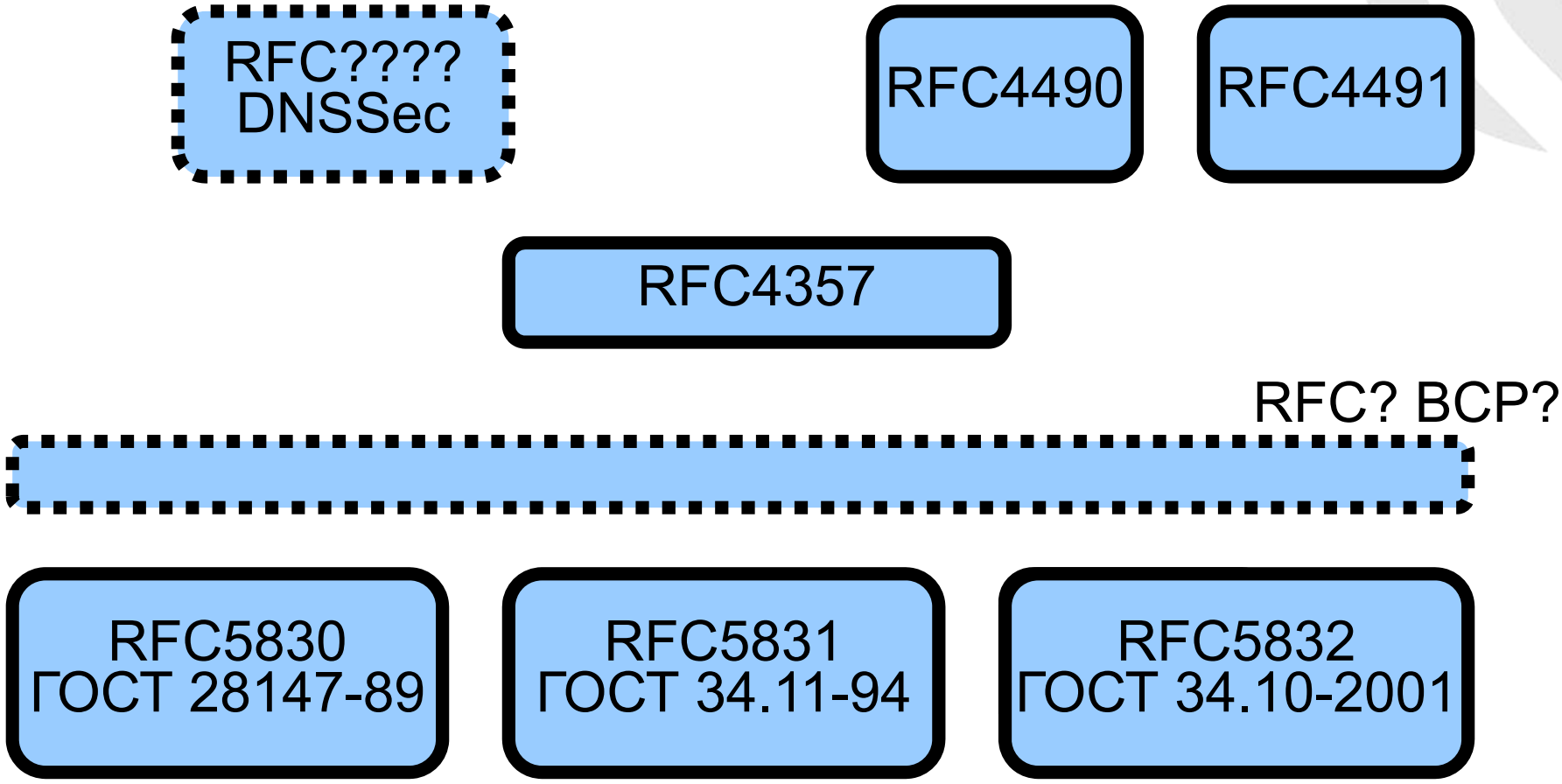
криптоком

Roadmap ГОСТ в DNSSec



криптоком

Структура ГОСТ RFC



криптоком

Спасибо за внимание!

Долматов Василий Вадимович
ООО “Криптоком”
Заместитель генерального директора
Тел. (499) 124-6226
E-mail: dol@cryptocom.ru
Web: www.cryptocom.ru

криптоком