Alibaba Cloud | Worldwide Cloud Services Partner

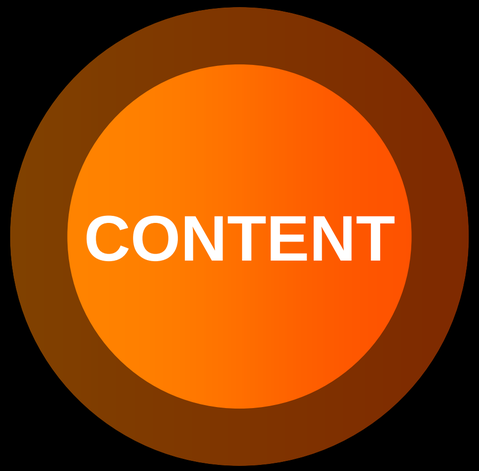
Alibaba DNSSEC Experience

Linjian (Davey) Song
Senior DNS Architect
linjian.slj@alibaba-inc.com

ICANN68 Tech Day

Content

Alibaba Cloud | Worldwide Cloud Services Partner

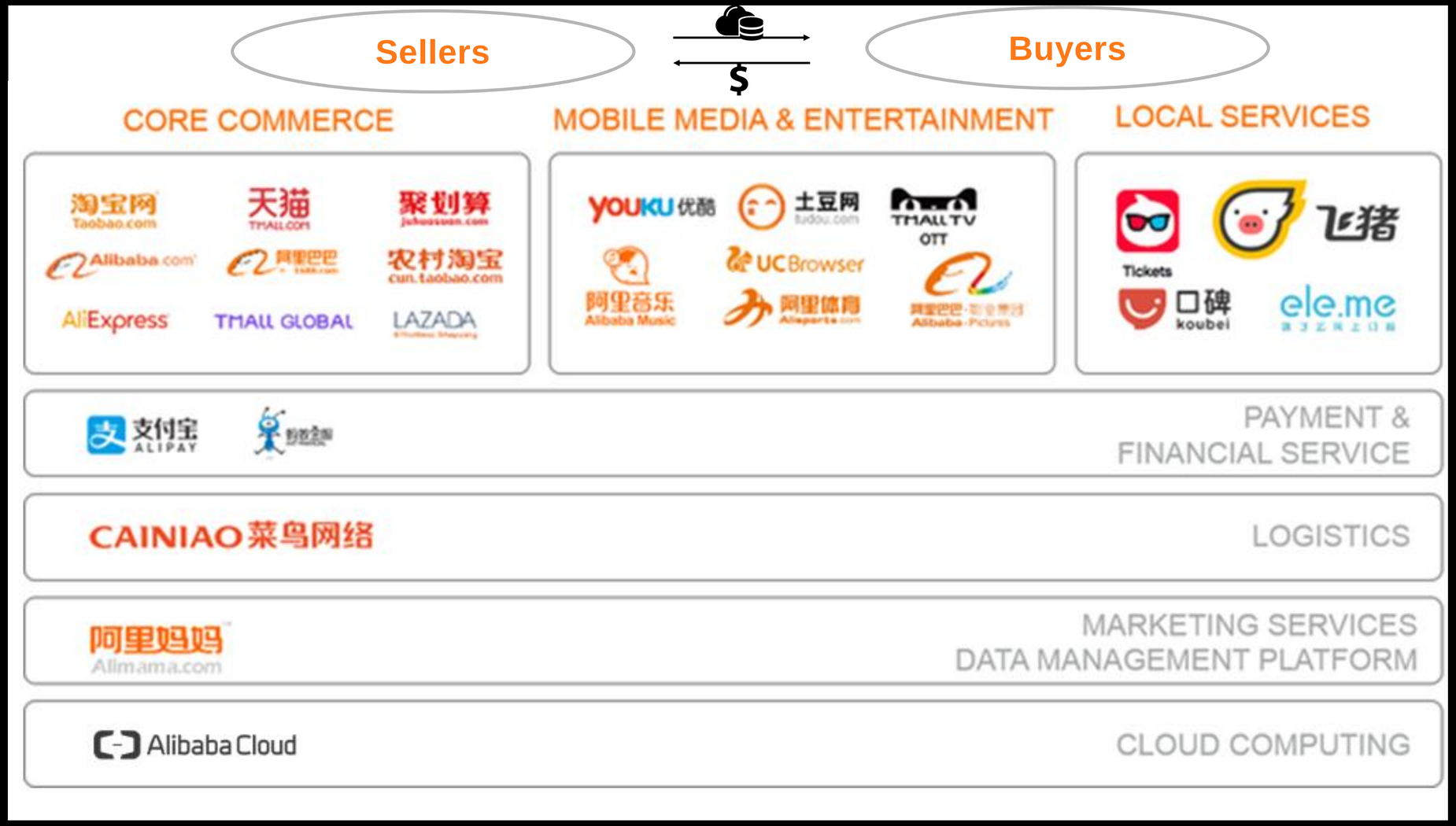


- Who are we ?
- DNSSEC in Alibaba Cloud
- Thoughts and Takeaway

Alibaba Ecosystem

Alibaba Cloud | Worldwide Cloud Services Partner

Alibaba's mission : To Make it Easy To Do Business Anywhere

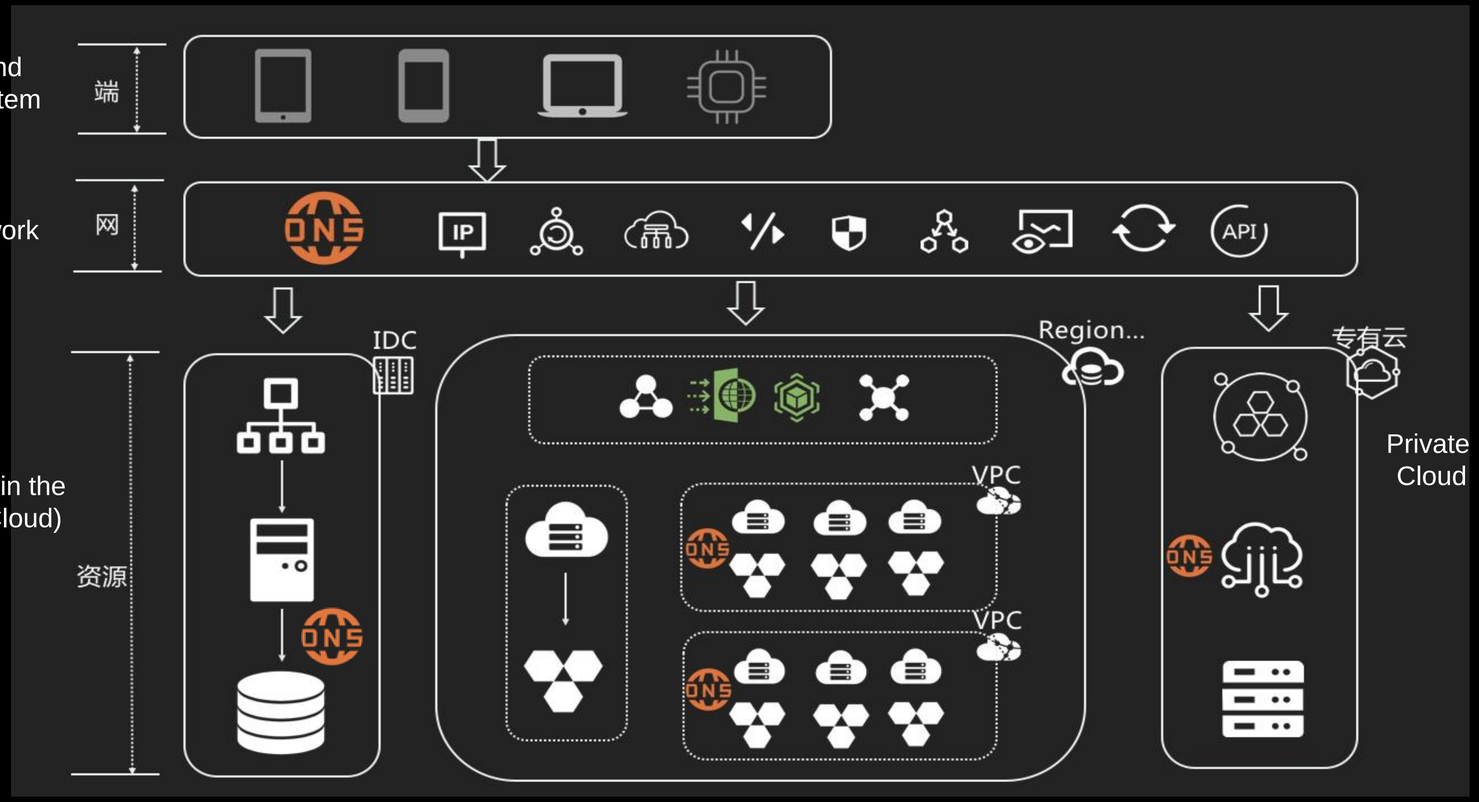


Tow numbers of 2019 "Double 11" Festival: 38.3 billion GMV(USD), up to 544 k/s transaction

Alibaba Cloud DNS – the Role and Challenges

Alibaba Cloud | Worldwide Cloud Services Partner

Alibaba Cloud DNS is a highly available and scalable Domain Name System (DNS) that provides authoritative DNS servers and DNS management services.



Challenges

Huge size and scale

(Serve ~1 billion users, 700 billion queries per day（RNDS+ADNS）, serve 20 regions and Millions VMs)

+

- High Performance (QPS)
- High availability (SLA)
- Accurate traffic scheduling and load balance (multi-policies)

So it is **very prudent** to deploy new technologies considering HA and risk management

What we do DNS in Alibaba Cloud

Alibaba Cloud | Worldwide Cloud Services Partner

Provide Managed DNS and GEO DNS in various networks and scenarios

Managed DNS / Authoritative DNS

Hosting **20 million** zones

Inner DNS for VPC

10,000 PVT-Zones

Global traffic Management

for failover and recovery

ASD (Apsara Stack DNS)

DNS in Private Cloud

Alibaba Cloud DNS is the largest DNS provider in Asia

More Capacities

Alibaba Cloud | Worldwide Cloud Services Partner

Alibaba Cloud DNS developed the advance services based on customers' requirements

Authoritative DNS in June 2018

Public DNS in Oct 2019

Alibaba Public DNS: www.alidns.com

Online in Jan 2020

For DNS data integrity

Supporter of DNS Flag Day

Public DoH/DoT in April 2020

Consideration on Data privacy and security

Alibaba Public DNS: www.alidns.com

Concerns and Challenges on DNSSEC

Alibaba Cloud | Worldwide Cloud Services Partner

Issues on DNSSEC adoption status and value added

- DNSSEC is not fully deployed in DNS resolvers globally
- Names of Large Internet companies, google.com, facebook.com, apple.com, amazon.com has not been signed today
- DNSSEC only provides authentication of data integrity, not a full solution against DNS hijack

Issues on implementation and operation

- DNSSEC Signing at Scale - lack of experience and know-how
- Integration of existing infrastructure - Impact and risk control
- Concerns on Poor Performance of DNSSEC signing – Require extra investment on the existing system

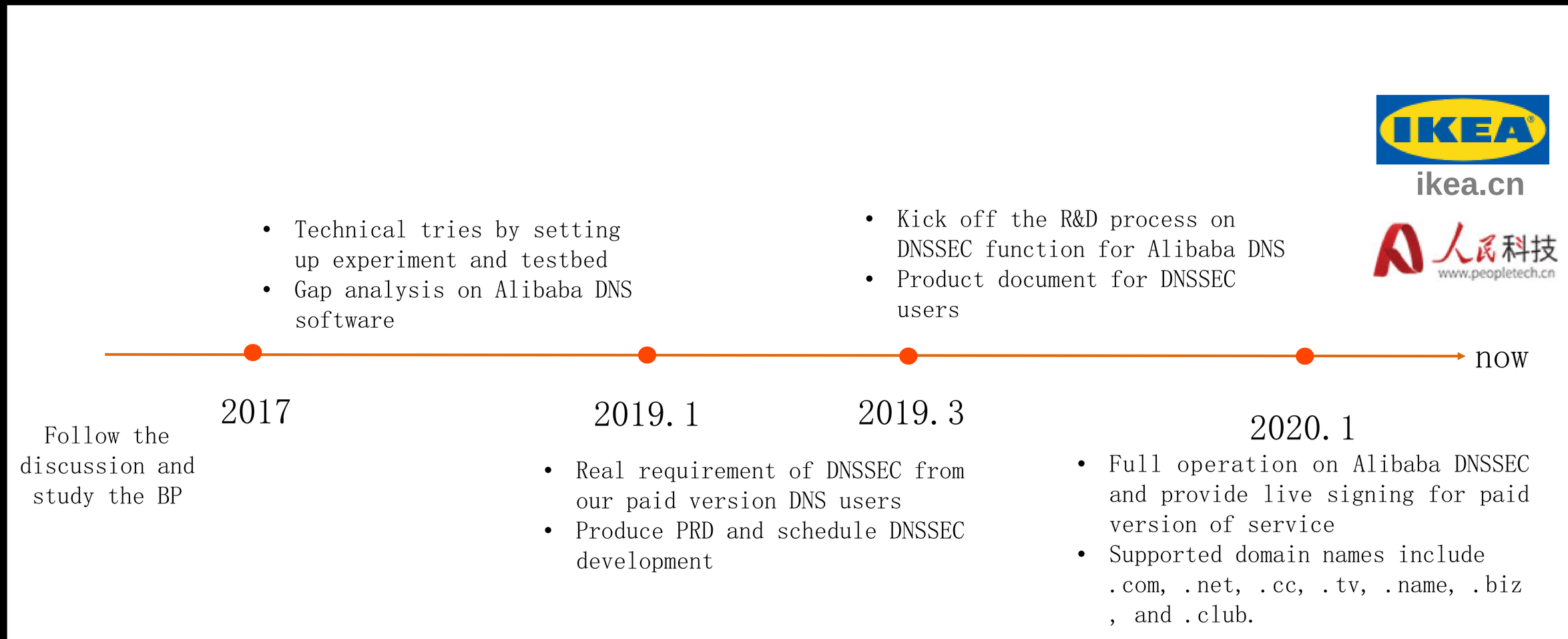
Two Reasons to deploy DNSSEC

Alibaba Cloud | Worldwide Cloud Services Partner

- From the business sense, customers ask for DNSSEC and our rivals start to deploy DNSSEC
- From the technical sense, DNSSEC provides a check for data integrity. It adds value to the domain and DNS as an Internet authoritative directory

History of DNSSEC in Alibaba Cloud

Alibaba Cloud | Worldwide Cloud Services Partner

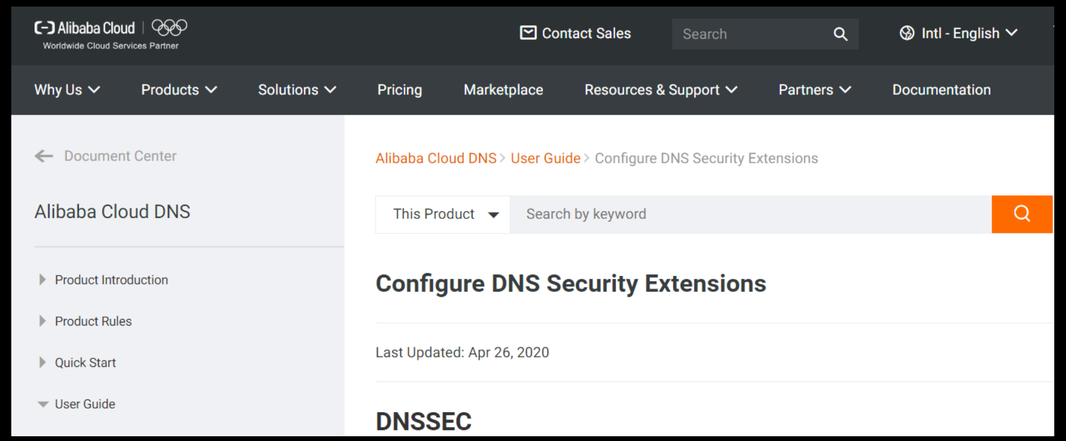


Configure DNSSEC in Alibaba DNS

Alibaba Cloud | Worldwide Cloud Services Partner

1. The login [Cloud resolution DNS console](), and follow the guide to DNSSEC setting page and click the button

2. Copy DS record information such as Key Tag, Algorithm, Digest Type, Digest, and then add a DS record to the domain registrar.

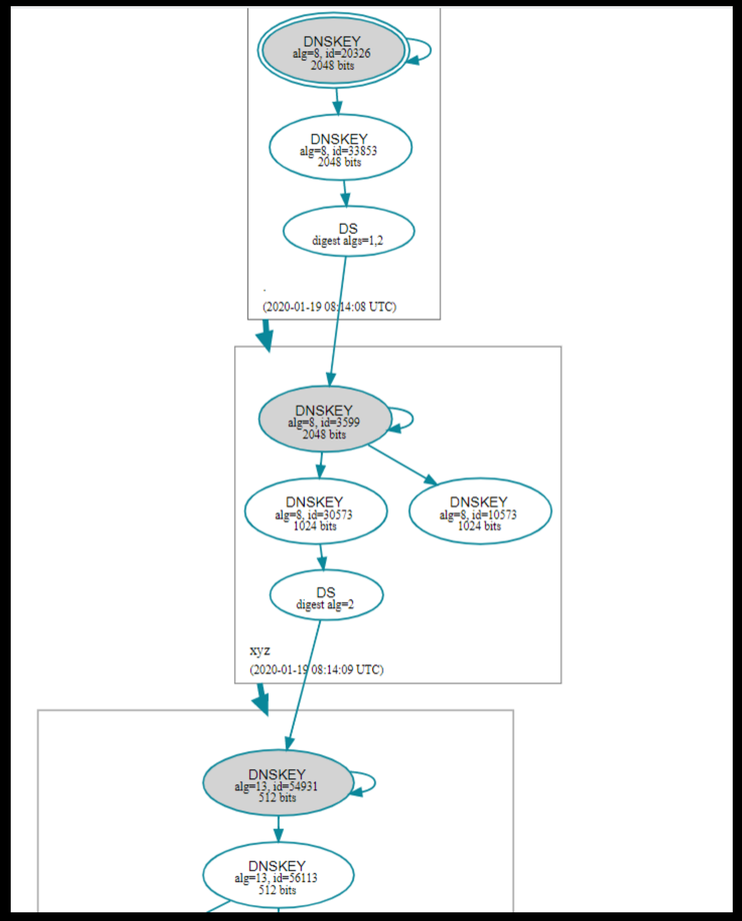


https://www.alibabacloud.com/help/doc-detail/149662.htm

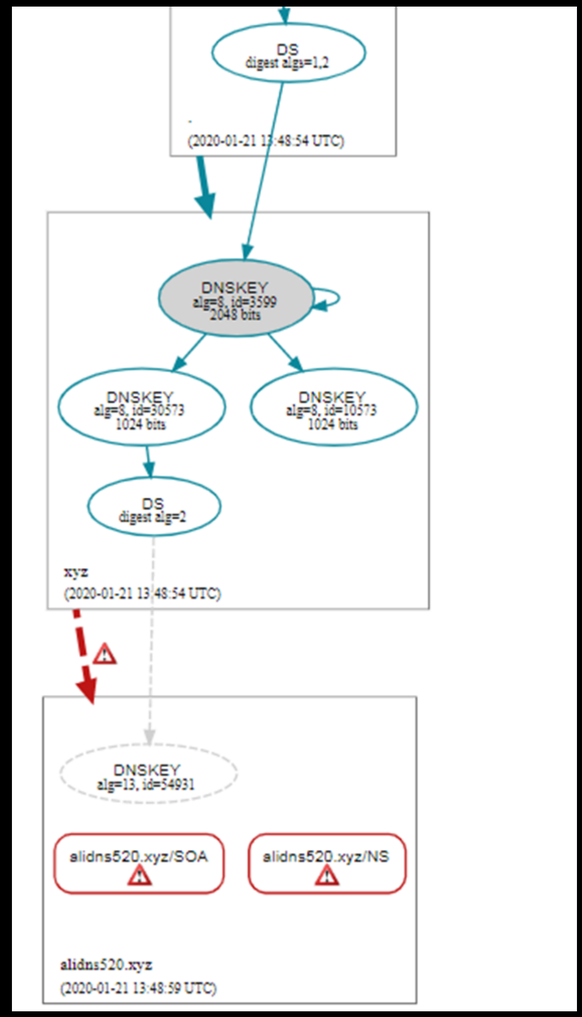
DNSSEC effectiveness test method

Alibaba Cloud | Worldwide Cloud Services Partner

Recommend dnsviz.net to Check whether DNSSEC is on or not



DNSSEC active



DNSSEC inactive

Technical overview in one slides

Alibaba Cloud | Worldwide Cloud Services Partner

- **Live signing for zones which enable DNSSEC**
- **Deploy ECDSA P256/ SHA256**

  ECC has smaller keys/signature, faster signing and better key strength

- **NESC for negatives**
- **Global ZSK and KSK**
- **Alibaba's KMS for Key management**
- **Key Pre-publish for ZSK rollover – to reduce the time of live signing**

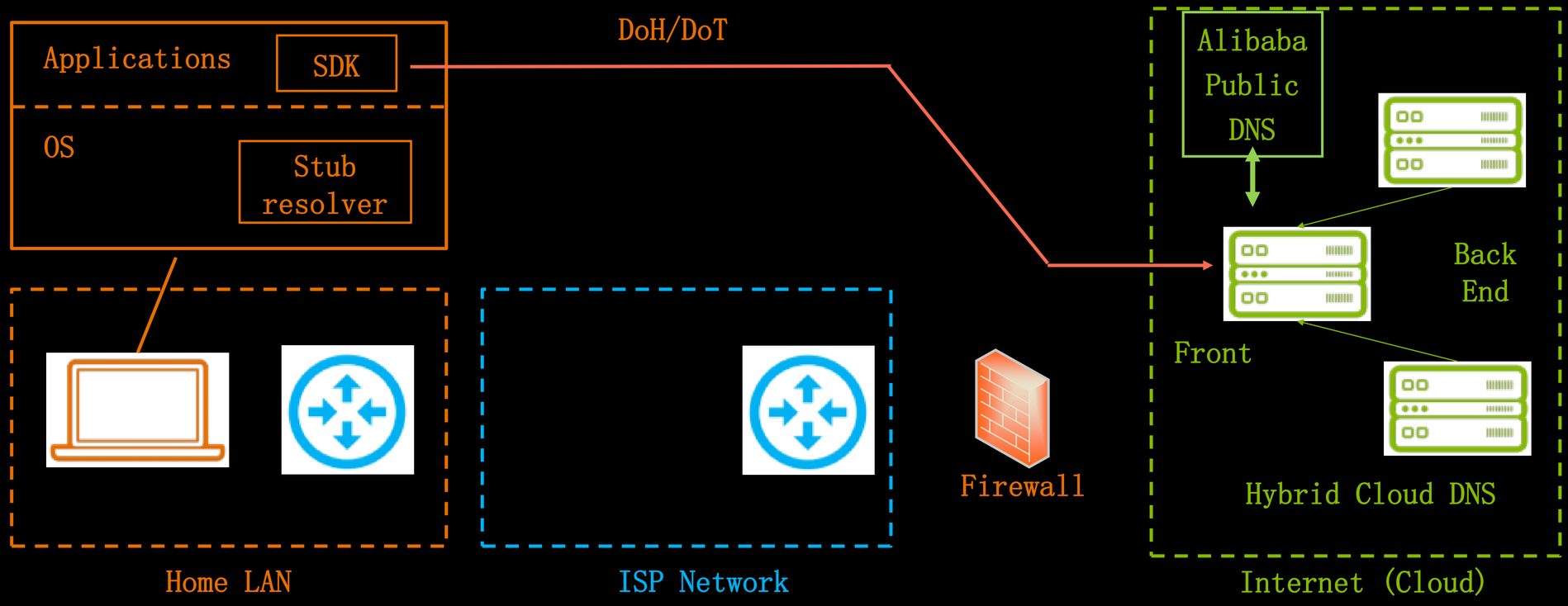
Acknowledgement to Cloudflare's best practice on DNSSEC

https://indico.dns-oarc.net/event/21/contributions/297/attachments/265/484/DNSSEC_live_signing_at_scale.pdf

DoH/DoT VS. DNSSEC?

Alibaba Cloud | Worldwide Cloud Services Partner

We provide Public DoH/DoT for DNS privacy, to avoid interference from third party network and DNS hijacking



- Provide SDK for APP developers to enable the app do the DNS in application level

  Requirement on accurate Geolocation, avoid DNS hijacking, very short propagation time, gated launch etc.

Note: DOH/DOT is a not replacement of DNSSEC , although they have similarity function against DNS hijack

Some Thoughts during DNSSEC deployment

Alibaba Cloud | Worldwide Cloud Services Partner

Factors of a successful DNS technology and adoption

- To meet real market demand and creating more customer value
- To fit the evolution of Infrastructure Technology

  ADD, Edge Computing, IoT, Mixed network scenarios
- To Internet governance policy enforcement

  Privacy, encrypted DNS. etc

Experience and Takeaway

Alibaba Cloud | Worldwide Cloud Services Partner

- Good understanding of DNSSEC and your users' requirement
- There are similarity between DoH/DoT and DNSSEC, but they fit different purpose and chosen by different customers
- Follow and test the Best Practice of DNSSEC which fits your situation
- Full preparation for DNSSEC operation as a business
    - DNSSEC implementation in large scale
    - Integration with your existing infrastructure
    - Full experiments and tests if not ready
    - SLA and expected traffic load
    - Failure over solution
    - Help Docs and Customer Service for DNSSEC

Alibaba Cloud | Worldwide Cloud Services Partner