TLS and TLSA

Bindhumadhava B S & Balaji R

Computer Networks and Internet Engineering Group
Centre for Development of Advanced Computing
No. 68, Electronics City, Bangalore 560100

ICANN 57, Hyderabad
5th November, 2016

C-DAC

- Centre for Development of Advanced Computing)
  - A premier Research institution under MeitY, GoI
  - 11 locations; Spread across the Nation;
  - Working on the entire gamut of IT
  - C-DAC Bengaluru:
    - Research Areas:
      - Cyber Security Research, Cloud and HPC, Language and ICT
    - Computer Networks & Internet Engineering Group:
      - Perimeter Security Solutions: UTM, Network Management tools
      - Information Security: Digital Signatures & PKI
      - Internet Standards: Awareness Generation and Contributions to Internet Protocols
      - DNS Security: Associated with ICANN since 2013

Agenda

- Drawing Synergies
  - TLS
    - Certificate Validation
    - Trust Stores
  - TLSA
    - Intro on DNSSEC and DANE
    - Issues

TLS

- Widely used Internet Security Protocol !
- Structure of TLS
  - Handshake Protocol
    - Establish Shared Keys & Authenticate Server and/or Client
    - Negotiate algorithms, modes, parameters
  - Record protocol
    - Carry individual messages, encrypted by Shared Keys (Symmetric)
  - Cipher Suites
    - Algorithms for Key Exchange, Authentication, Encryption, and MAC
- Objectives of TLS 1.3
  - Clean up, Increase Security; Improve Performance
- Certificates are the key!

Certificate Validation

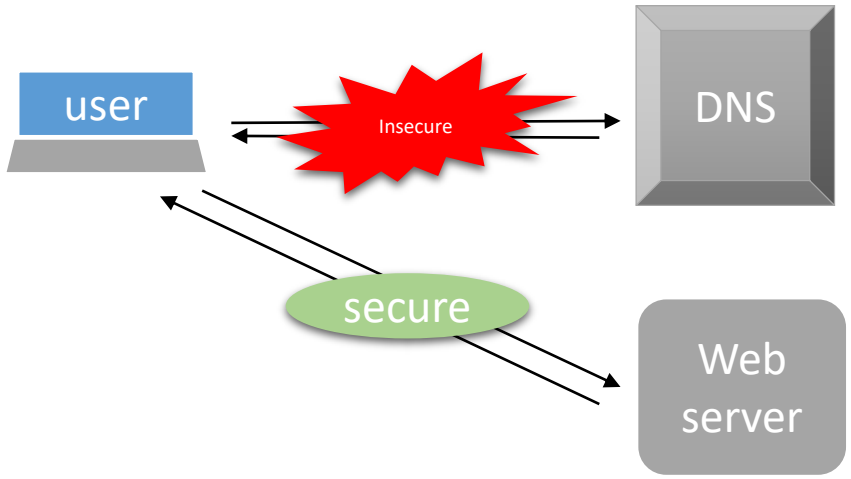
- A Complex Activity!
  - Algorithm in Brief
    1. Check for Validity (Time, CRL (except for root), Format) of Certificate
    2. Check and Validate the Signature in the Certificate using the issuer's certificate (which contains the public key) – including the CPS (Policy)
    3. If the issuer's certificate is not a self-signed certificate, then continue with this certificate from Step 1
    4. If it is a self-signed certificate,
       - Check if the Certificate is present in trust stores (Trusted Root CA)
         - If present, trust it and exit (allow user to proceed further)
         - If not prompt the user to take a decision to trust it or leave the site

Trust Stores

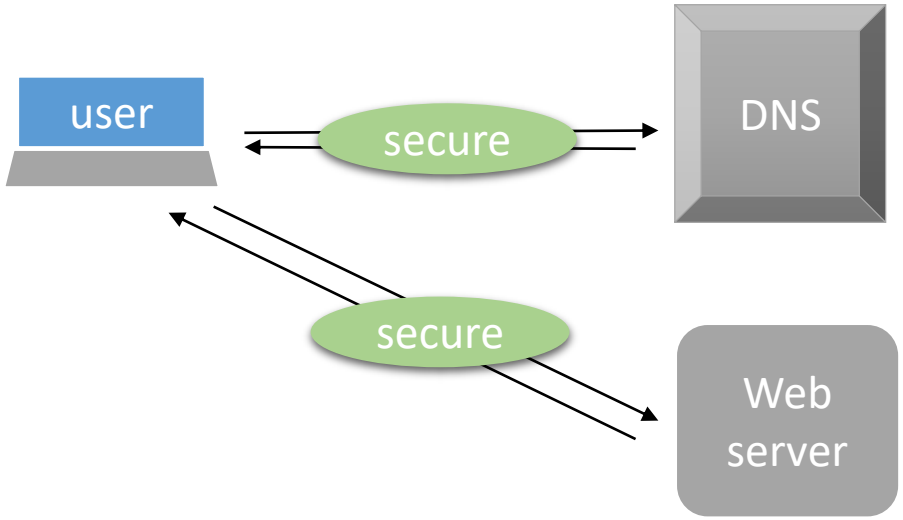
- Applications manage their own trust stores
  - and come up with a set of pre-loaded certificates
  - User have to explicitly add certificates of a domain they trust, but not present in trust stores

DNSSEC

Without DNSSEC



With DNSSEC

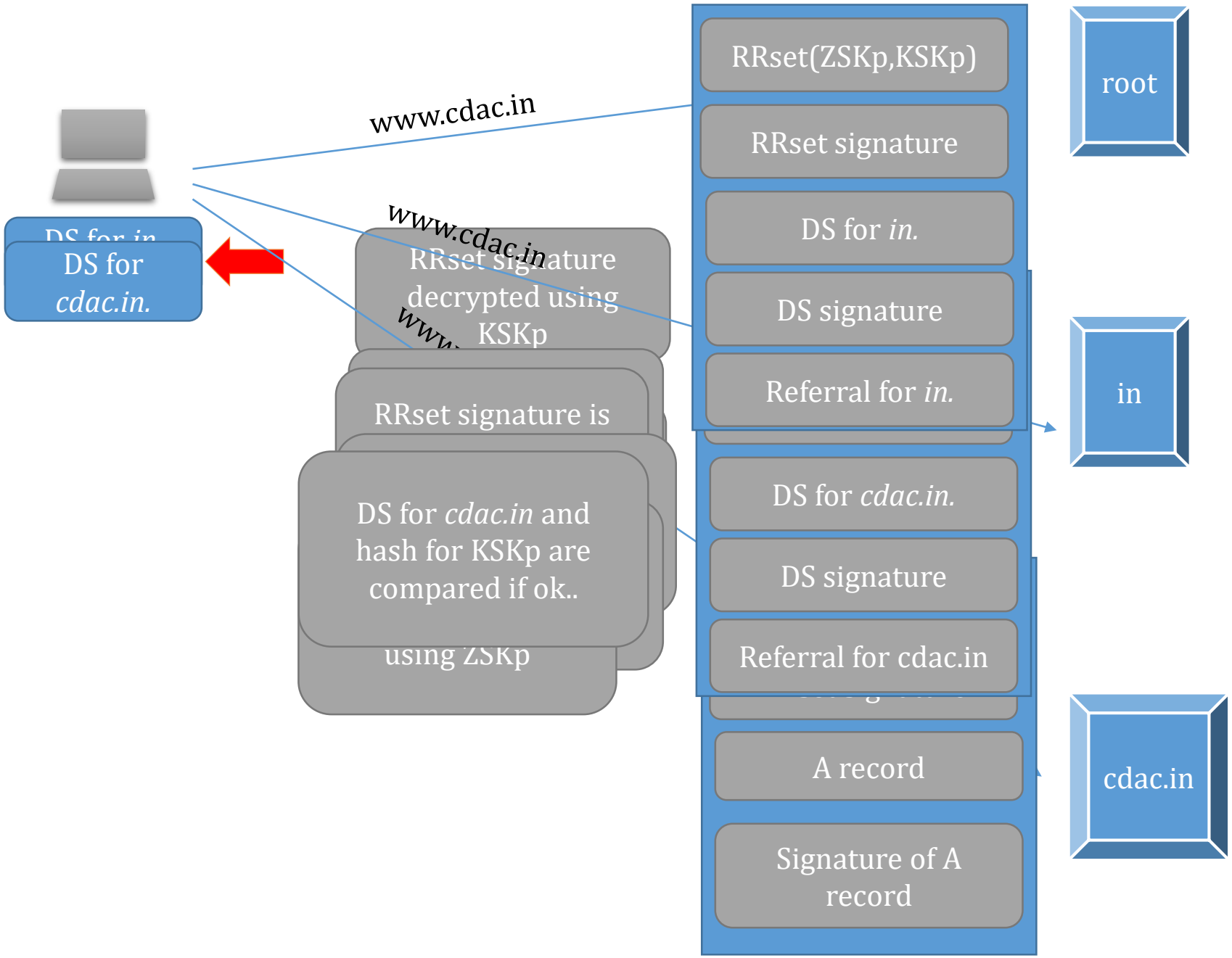


DNSSEC – Gentle Intro

- Each Zone will have two crypto key-pairs
  - Operational keys, called Zone Signing Key (**ZSK**)
    - Sign and validate the zone records and itself;
    - Public key is stored in the **DNSKEY** record
    - Private key is typically kept safe in HSM
  - Authenticators for the operational keys called as Key Signing Key (**KSK**)
    - Sign the ZSK at the apex of the zone
      - Signs only the DNSKEY RRset
    - Public key becomes a DNSKEY at zone apex
- Delegation Signer
  - Represented by a Delegation Record
  - Contains the hash of KSK which resides inside parent zone

DNSSEC Summary

- DNSSEC uses Public Key Cryptography and digital signatures to provide
  - Data Origin Authentication
    - Did the DNS reply really come from the zone? (Say *.com*)
  - Data Integrity
    - Did an attacker modify the data in the response, since it was signed?
- DNSSEC
  - Provides protection against spoofing of DNS Data
  - does not provide confidentiality / secrecy for DNS data
  - does not protect against Denial of Service attacks


www.cdac.in
DS for
cdac.in.
www.cdac.in
RRset signature
decrypted using
KSKp
RRset signature is
using ZSKp
DS for cdac.in and
hash for KSKp are
compared if ok..
RRset(ZSKp,KSKp)
RRset signature
DS for in.
DS signature
Referral for in.
DS for cdac.in.
DS signature
Referral for cdac.in
A record
Signature of A
record
root
in
cdac.in

DANE

- DNS-based Authentication of Named Entities
- Allows pinning of TLS Certificates into DNSSEC Zone – TLSA

TLSA

```
_443._tcp.www.rahul.com. IN TLSA ( 03 01 01 776195babe2b2309e67ffb3b30cd49f9a448
5b609b2b1bf08f1c9a15fb427127 )
```

- TLSA
  - Validation of target certificate Vs certificate from DNS
    - CA in the browser is checked with Certificate from DNS
    - Certificate from target matches with Certificate from DNS
    - CA may not be listed in the Trust Stores
    - May be using a Self-signed Certificate (03)
- Risks
  - Allows self-signed Certificates to be pinned to a domain
  - Probable Attacks such as Unknown Key Share (UKS) has been identified (Internet Draft published on Oct 9, 2016)

Summary

- TLS and TLSA (DANE) are both required to establish secure and **reliable** communications
  - Despite the complexities involved in them!

References

- Certificate Validation - RFC 5280
- DANE – RFC 6698, RFC 7671
- https://www.ietf.org/id/draft-barnes-dane-uks-00.txt