Strengthening the Ecosystem of Digital Trust

Dr. Balaji Rajendran

Scientist 'F'

Resilient Information Systems and Engineering (RISE)

Centre for Development of Advanced Computing (C-DAC)

Bangalore

CA/B Forum #61, New Delhi

26th February 2024

Contents in Brief

- Digital Trust
- Trust Scores
  - TLS, DANE, Domain, Content
- Leveraging AI for determining Trust Scores
- Indian Web Browser Development Challenge

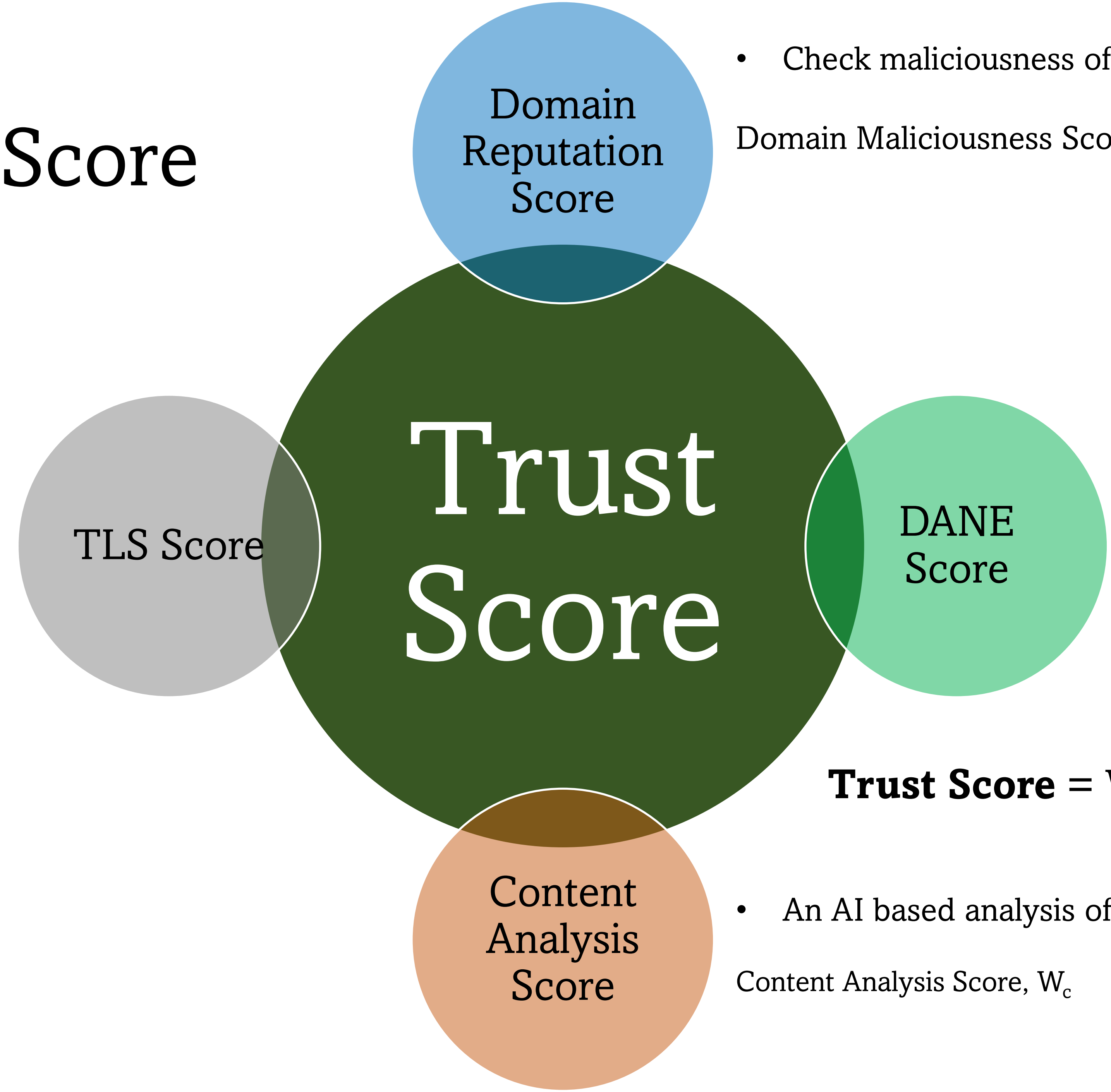
Digital Trust

- An encapsulated ring of ‘trust’ within the vast untrusted universe, comprising of:
  - Trusted Entities & Trusted Communications
  - Assurance of all security and privacy properties in the transactional workflows among ‘trusted’ entities.

Trusted Browsing

- End-to-End Assurance from Domains Names to Content
- Facilitate standard Plug-ins exclusively for ‘Trust Scores’
- Preferably on the Address Bar
- Trust Scores could be derived from the following:
  - TLS Score
  - DANE Score
  - Domain Reputation Score
  - Content Analysis Score

Trust Score



Domain Reputation Score

TLS Score

Trust Score

DANE Score

Content Analysis Score

- Check maliciousness of domain name

Domain Maliciousness Score W_d

- Verify Certificate Expiry (V_c)
- Verify if the domain name or IP address in certificate matches the server's information (V_s)
- Verify CA information (V_a)

TLS Score, $W_t = V_c + V_s + V_a$

- Certification verification and Domain Verification

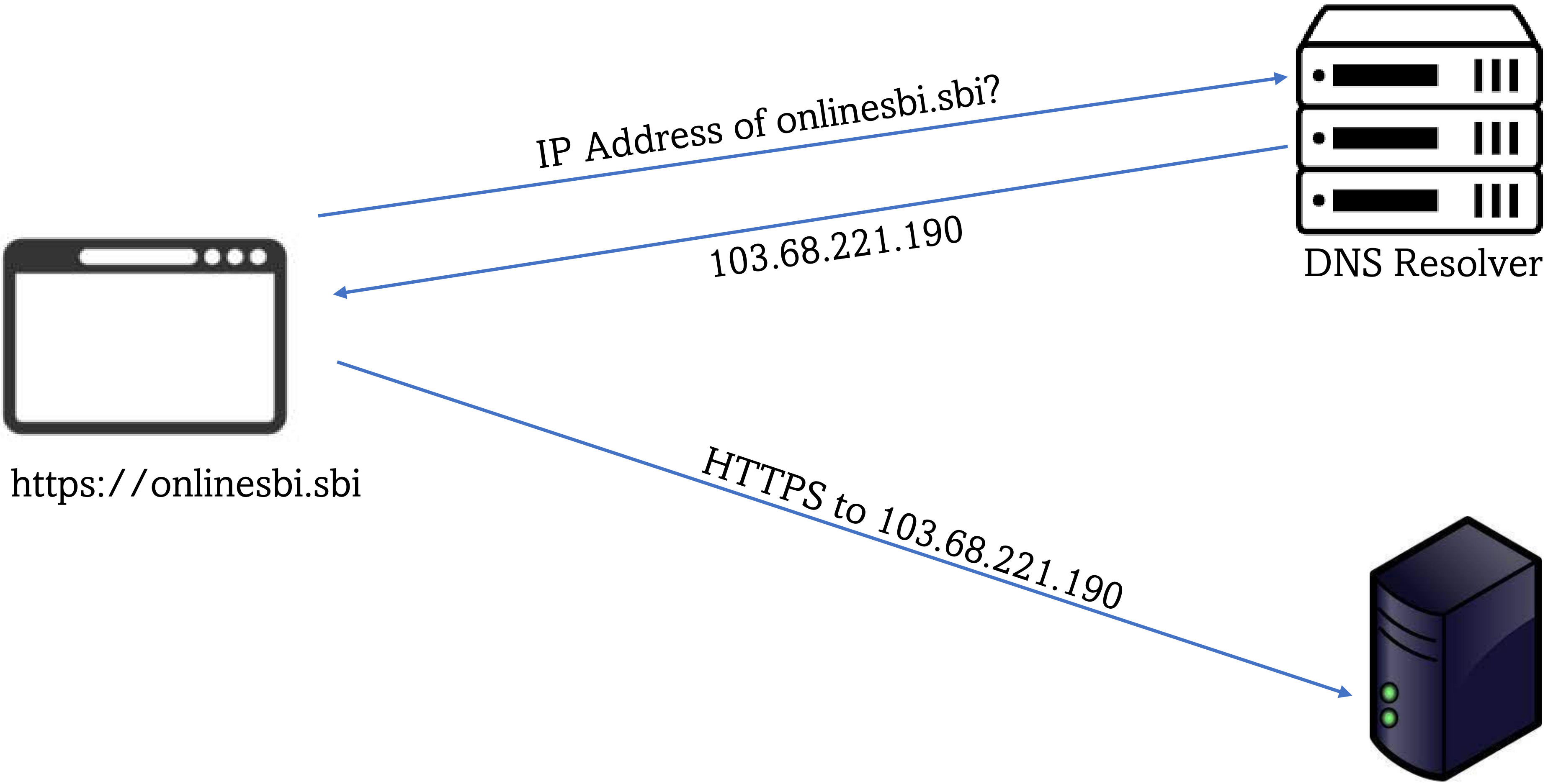
DANE Score, W_a

Trust Score = $W_t + W_d + W_a + W_c$

- An AI based analysis of website content

Content Analysis Score, W_c

Connecting to a Website



How to trust that 103.68.221.190 is the right website for onlinesbi.sbi?

TLS Certificates and Trust Stores - Challenges

- Security is as weak as the weakest link in the Chain
- Browsers depend on Trust Stores
- An exploited CA can compromise the whole ecosystem

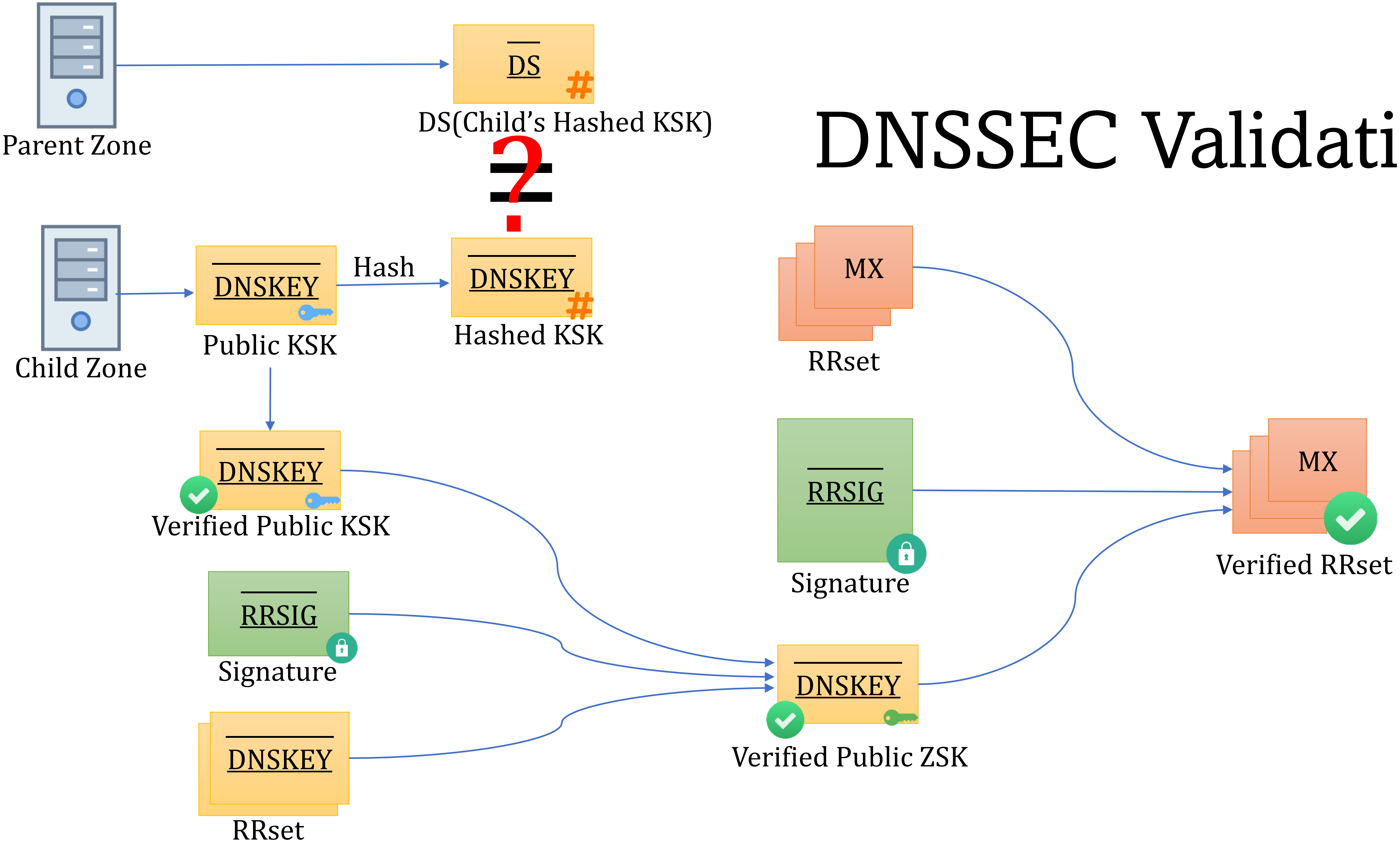
Solution - TLS-DNS Ecosystem of Trust

- Root-of-Trust Ecosystems of TLS & DNS can be combinedly leveraged to strengthen the trust factor
- DNS
  - Get the certificate from DNS lookup
  - Get the issuer CA information
  - Get the Hash of Certificate
  - Get the Public Key

DNSSEC (Briefly)

- DNSSEC signs DNS replies
  - Uses public-key cryptography to sign responses
- It guarantees:
  - Authenticity of DNS answer origin
  - Integrity of reply
  - Authenticity of denial of existence
- It does not
  - Provide confidentiality for DNS data
  - Protect against Denial of Data

DNSSEC Validation



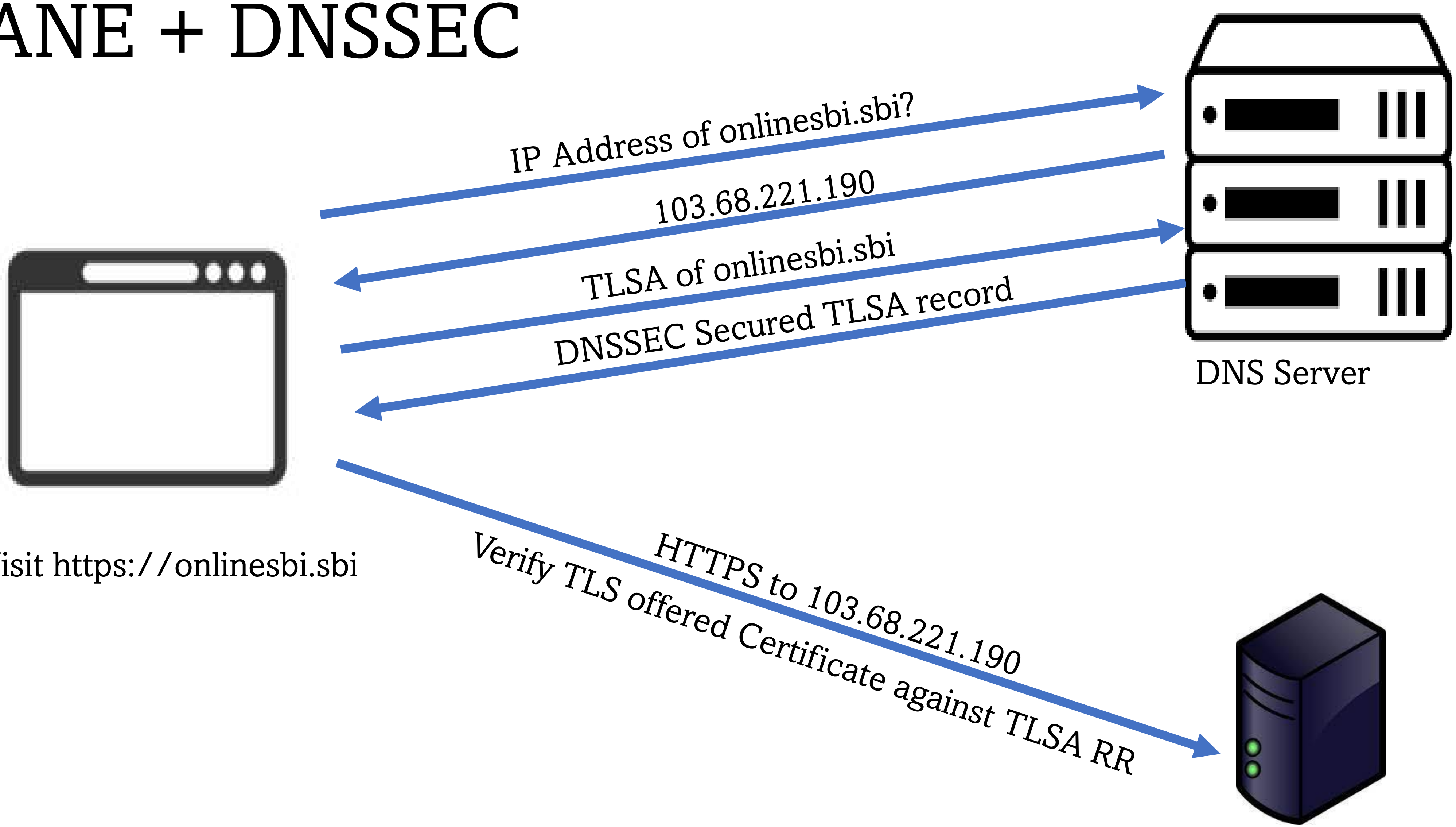
DANE

- DNS Based Authentication of Named Entities
- Administrators publish certificate information using TLSA records in the DNS
- Clients can query that info using DNSSEC (prevents TLSA falsification)
- Spoofed certificates can be detected.
- Revoking certificate -> Remove TLSA record
- TLSA can be easily generated using OpenSSL

TLSA RR

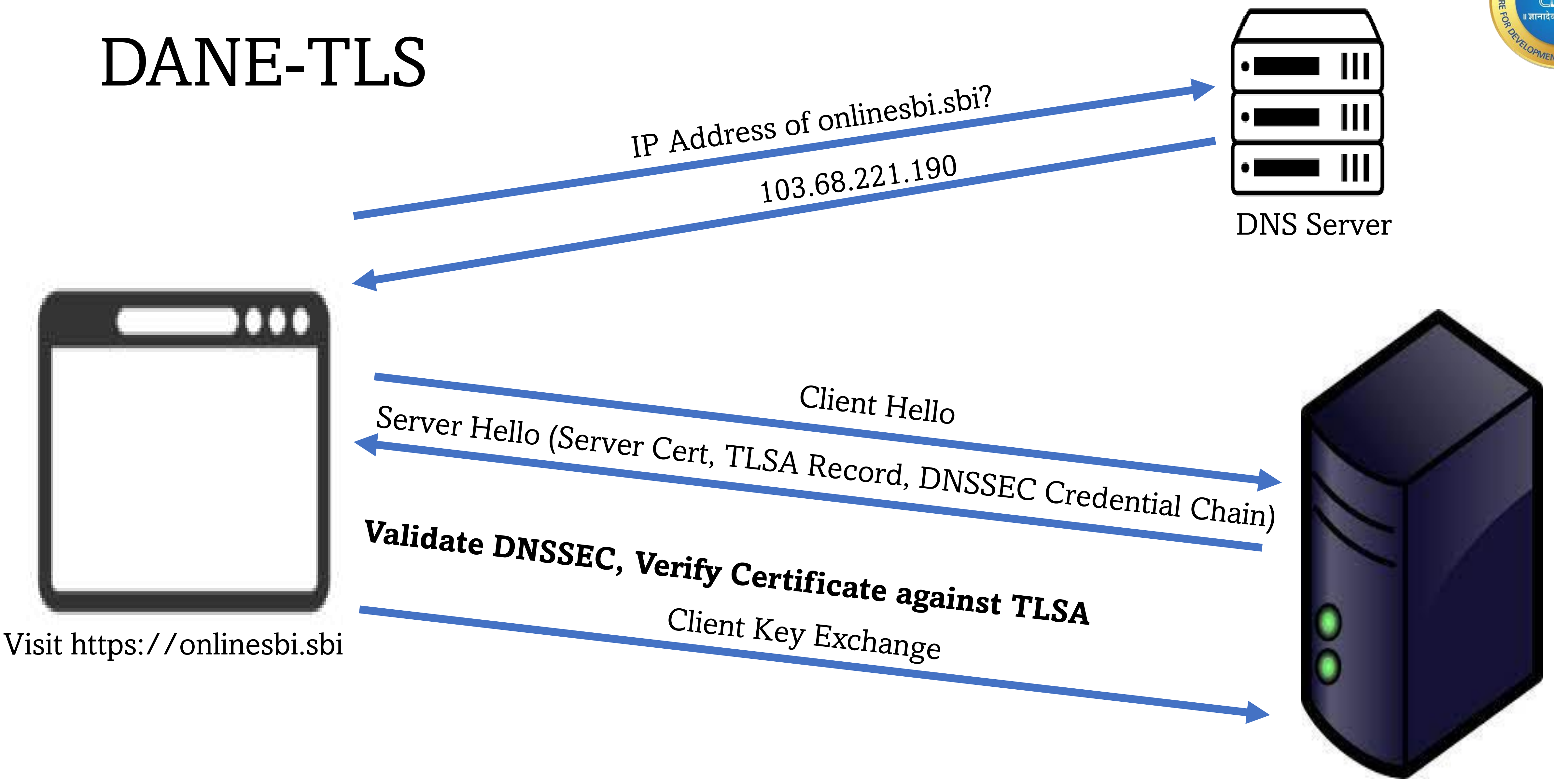
- Usage: (From 0 to 3) It specifies the provided association that will be used to match the certificate presented in the TLS handshake.
  - CA Specification
  - Certificate Specification (End Entity)
  - Trust Anchor Specification
  - Domain-issued Certificate (Self-Signed)
- Selector: (From 0 to 1) It specifies which part of the TLS certificate presented by the server will be matched against the association data.
  - Full Certificate
  - SPKI (Subject PKI) – Public Key and other associated information
- Matching-Type: (From 0 to 2) It specifies how the certificate association is presented
  - No hash
  - SHA2-256
  - SHA2-512
- Data Field: Full Value or Hash value.

DANE + DNSSEC


IP Address of onlinesbi.sbi?
103.68.221.190
TLSA of onlinesbi.sbi
DNSSEC Secured TLSA record
DNS Server
Visit https://onlinesbi.sbi
HTTPS to 103.68.221.190
Verify TLS offered Certificate against TLSA RR

Will multiple DNS queries slow the access?

DANE-TLS



DNS Server

IP Address of onlinesbi.sbi?

103.68.221.190

Visit https://onlinesbi.sbi

Client Hello

Server Hello (Server Cert, TLSA Record, DNSSEC Credential Chain)

Validate DNSSEC, Verify Certificate against TLSA

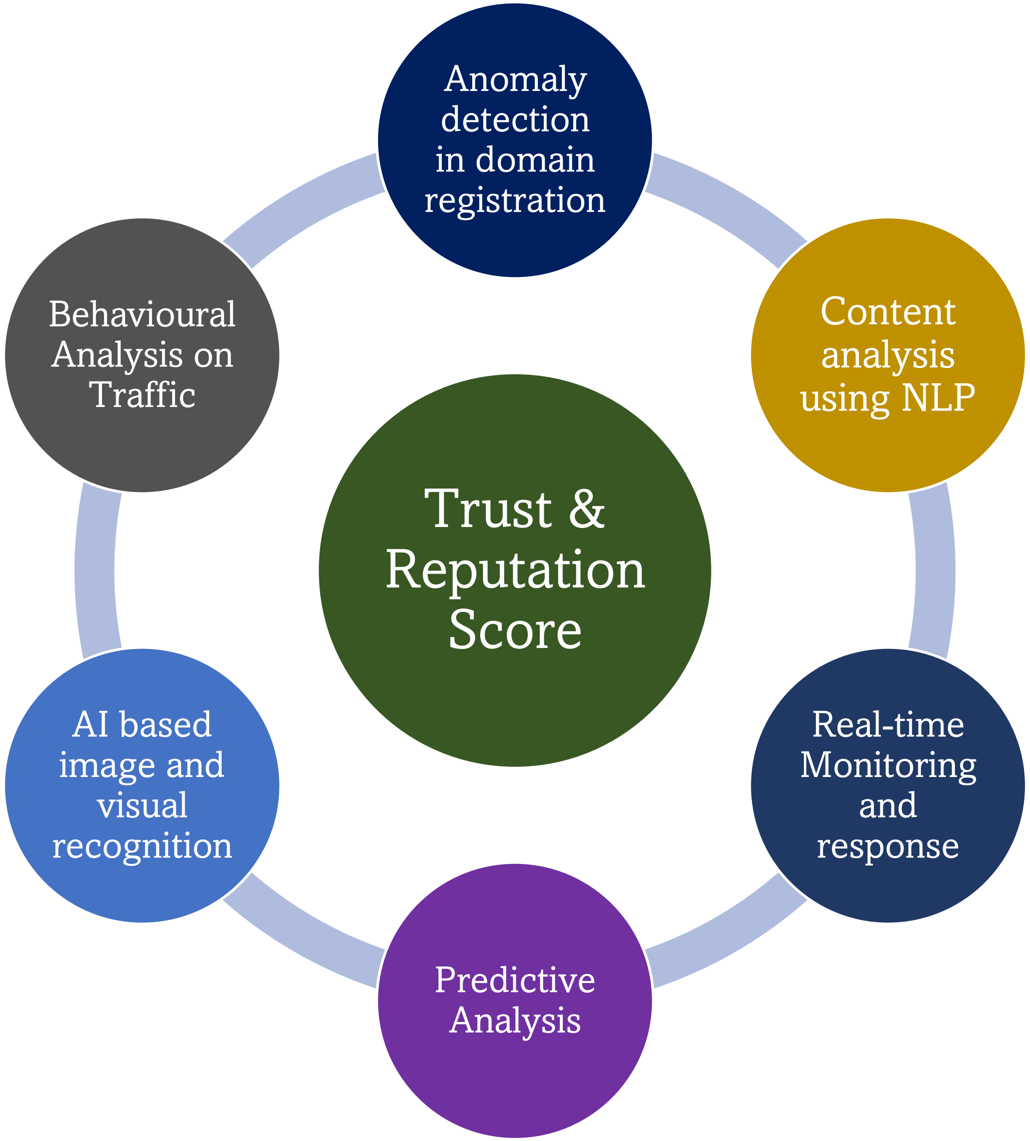
Client Key Exchange

Challenges

- Browser Support
  - DANE+DNSSEC will make browsers slow, maybe.
  - Same through plugin/extension
- DNSSEC Validation
  - Only 31% (https://stats.labs.apnic.net/dnssec/XA)

Domain Reputation & Content Analysis

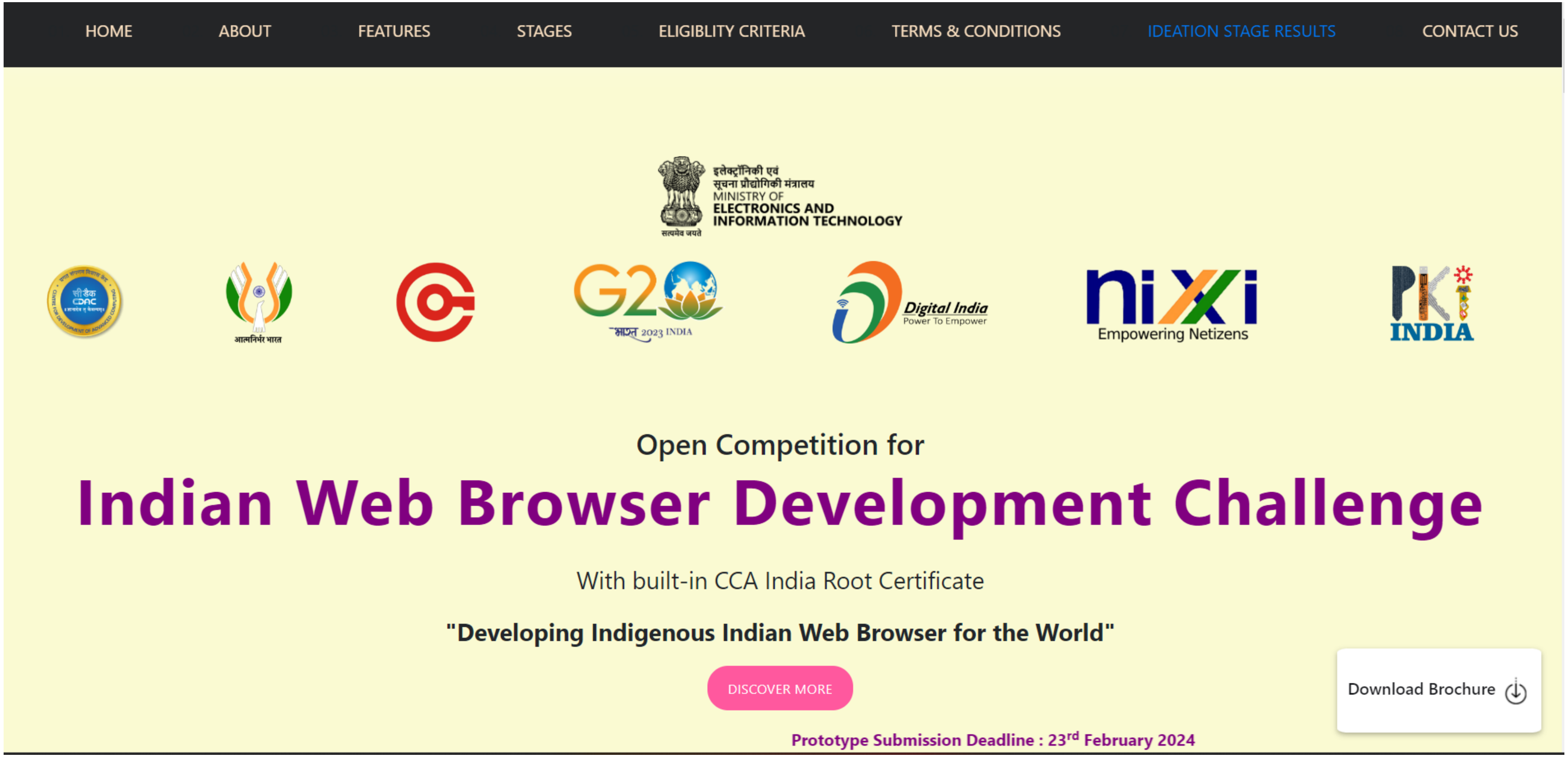
- VKYC (Video-based Know Your Customer) can improve trust-worthiness of registered domain
- Deployment of Domain Anchors at Internet Exchange Points to monitor and measure traffic can help in:
  - Detecting malicious domains including the one’s using DGA
  - Assist in developing reliable trust scores for domains


Anomaly detection in domain registration
Content analysis using NLP
Real-time Monitoring and response
Predictive Analysis
AI based image and visual recognition
Behavioural Analysis on Traffic
Trust & Reputation Score

Indian Web Browser Development Challenge

- To develop a browser loaded with features for:
  - Digitally signing documents within the browser using DSCs in Crypto Tokens
  - Support searching, accessing Indian IDNs
  - Support Web3 Features
  - Support Child-Friendly Browsing Options
  - Support Examination Mode
- Multi-Stage Competition;
- Encouraging Industry, Startups and Innovators to deliver

Web Portal (https://iwbdc.in)



Open Competition for

Indian Web Browser Development Challenge

With built-in CCA India Root Certificate

"Developing Indigenous Indian Web Browser for the World"

Prototype Submission Deadline : 23rd February 2024

Summary

- Explicit Communication of Trust to users could alert the users
- Trust Score Factors: TLS, DANE, Domain Names, Content Analysis
- AI can be leveraged in maliciousness prediction of domain names and contents
- Trust Score – Standard Plugins - can strengthen the Ecosystem of Digital Trust

Thank You

balaji@cdac.in