# Indian Web Browser Development Challenge

**For Prelims: Indian Web Browser Development Challenge, Controller of Certifying Authorities, Secure Sockets Layer,** Aatmanirbhar Bharat.

**For Mains:** Indian Web Browser Development Challenge.

**Source: PIB**

## Why in News?

Recently, the Ministry of Electronics & Information Technology (MeitY) has launched the **Indian Web Browser Development Challenge (IWBDC),** inviting developers to create an Indigenous Indian Web Browser for global use.

- A key requirement of this competition is that the browser ideas must trust the **Controller of Certifying Authorities (CCA)**, the Indian government's authority responsible for digital signatures, including **SSL (Secure Sockets Layer) certificates.**

## What is a Web Browser?

- The web browser is an application software to **explore** www (World Wide Web)**.** It provides an **interface between the server and the client** and requests to the server for web documents and services.
- It works as a compiler to render HTML which is used to **design a webpage.**
- Whenever we search for anything on the internet, the browser loads a web page written in HTML, including text, links, images, and other items such as stylesheet and JavaScript functions.
    - **Google Chrome, Microsoft Edge, Mozilla Firefox, and Safari** are examples of web browsers.

## What is the Indian Web Browser Development Challenge?

- **About:**
    - The IWBDC is an **Open Challenge Competition** that seeks to inspire and empower technology **enthusiasts, innovators, and developers from all corners** of the country to create an **indigenous web browser.**
    - **It will have its** own trust store with an inbuilt Controller of Certifying Authorities (CCA) India root certificate, cutting edge functionalities and **enhanced security & data privacy protection features.**
    - IWBDC is **spearheaded by MeitY, CCA and** C-DAC Bangalore.
    - The competition is **being organised and financed in collaboration** with the **IT Ministry'**s Research and Development division and the **National Internet Exchange of**

**India.**

- **Objective:**
  - Proposed browser will focus on **accessibility and user friendliness,** ensuring **built-in support for individuals** with diverse abilities.
  - Moreover, the **browser envisions the ability to digitally sign documents** using a crypto token, **bolstering secure transactions and digital interactions.**
- **Significance:**
  - The challenge marks a significant **stride towards an** Aatmanirbhar Bharat, designed to strengthen India's digital sovereignty through the development of the Indian Web Browser.
  - This challenge addresses one of the critical components – Web browser – through which the **end users accessing the Internet.**

## What are Secure Sockets Layer (SSL) Certificates?

- **About:**
  - An SSL certificate is a **digital certificate that authenticates a website's identity** and enables an encrypted connection.
  - It is a security protocol that creates an **encrypted link** between a **web server and a web browser.**
    - Companies and organizations need to add SSL certificates to their websites to **secure online transactions** and keep customer information private and secure.
- **Role of Root certifying Authorities in Trust:**
  - While India has a legally valid root certifying authority called the **Root Certifying Authority of India**, established in 2000 under the CCA, the certificates issued by it are **not widely recognized by popular web browsers.**
    - The CCA has established the **RCAI under section 18(b) of the IT Act** to digitally sign the public keys of CAs in the country.
    - The RCAI is operated as per the **standards laid down under the Act.**
  - This reliance on foreign authorities has raised concerns over **digital security and foreign exchange outflow.**
- **Issues with Indian SSL System:**
  - India lacks a root certifying authority that is trusted by **major browsers like Google Chrome**, Mozilla Firefox, and Microsoft Edge.
    - This has led to Indian government and private websites **obtaining SSL certificates from foreign certifying authorities.**
  - A notable incident involving the **National Informatics Centre (NIC)**, a CCA-approved organization responsible for hosting and maintaining various Union and State Government websites, underscored **trust issues in Indian certifying authorities.**
    - In 2014, browsers and operating systems stopped trusting India's CCA after the NIC was linked to issuing fraudulent certificates.
  - While NIC's authorization for SSL certificate issuance was revoked, the **trust in Indian certifying authorities remained compromised.**

**(a)** 1 only
**(b)** 2 and 3 only
**(c)** 3 only
**(d)** 1, 2 and 3

**Ans: (c)**

- Digital signature is not a record, and the identification of certifying authority is ascertained from the digital certificate, not digital signature. Hence, statement 1 is not correct.
- A digital signature is used to authenticate the identity of the sender of a message or the signer of a document, and not to serve as a proof of users' authenticity to access a website or information on the Internet. Hence, statement 2 is not correct.
- A digital signature is an electronic form of a signature that allows the recipient to trust the fact that a known sender sent the message and it was not altered in transit. Hence, statement 3 is correct. Therefore, option (c) is the correct answer.

## *Mains:*

**Q:** Discuss different types of cyber crimes and measures required to be taken to fight the menace. **(2020)**

**Q:** Discuss the advantages and security implications of cloud hosting of servers vis-a-vis in house machine based hosting for government businesses. **(2015)**

**Q:** What is a digital signature? What does its authentication mean? Give various salient built-in features of a digital signature. **(2013)**