Ministry of Electronics and
Information Technology
Government of India

Annual Report
(2018)

Indian Computer Emergency Response Team (CERT-In)

Ministry of Electronics & Information Technology

Government of India

Table of Contents

1. Highlights of 2018

1.1. **Summary of major activities**

a) CERT-In is in a strategic position as a Steering Committee Member in APCERT and also convening two working groups namely IoT Security and Secure Digital Payments.

b) In the year 2018, CERT-In handled **208456** incidents. The types of incidents handled were Website Intrusion & Malware Propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements, Unauthorized Scanning activities and vulnerable service. Remedial measures for handling incidents were suggested and implemented in coordination with relevant stakeholders.

c) CERT-In is keeping track on latest cyber threats and vulnerabilities. **193** security alerts, **36** advisories and **222** Vulnerability Notes were issued during the year 2018.

d) CERT-In conducted **24** cyber security training and awareness programs to Government, Public and Critical Sector organisations and communication & Information infrastructure providers to educate them in the area of Information Security with the latest security threats, needs and developments & deployment of techniques and tools in order to minimize security risk.

e) CERT-In participated as a player in **3** International cyber security drills and in **1** exercise participated as observer country.

1.2. **Achievements & milestones**

- Botnet Cleaning and Malware Analysis Centre ("Cyber Swachhta Kendra") was awarded as one of 51 "Gems of Digital India 2018" in June 2018. "Cyber Swachhta Kendra" also awarded "SKOCH Order-of-Merit and Gold Award" for Cost Effective Cyber Security Model in the month of December 2018. The centre is providing detection of malicious programs and free tools to remove the same for common users.

- Indian Computer Emergency Response Team is carrying out cyber security exercises comprising of table top exercises, crisis management plan mock drills and joint cyber security exercises with organizations from key sectors to enable participating organizations to assess their preparedness in dealing with cyber crisis situations. Total of 11 such exercises have been conducted in 2018.

- In 2018, CERT-In has signed Memorandum of Understandings (MoUs) on cyber security cooperation with two countries namely The Department of Information Communications Technology, The Republic of Seychelles and The Moroccan Computer Emergency Response Team (ma-CERT), National Defence Administration, The Kingdom of Morocco to enable information sharing and collaboration for incident resolution.
- CERT-In has set up its own automated Threat Information and Intelligence sharing platform for sharing Indicators of Compromise (IoCs) among some select stake holders.
- CERT-In has launched its Threat and Situational Awareness Project (TSAP) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

2. About CERT-In

2.1. **Introduction**

CERT-In is a functional organisation of Ministry of Electronics and Information Technology, Government of India, with the objective of securing Indian cyber space. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services.

The Information Technology Act, 2000 designated CERT-In to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Such other functions relating to cyber security as may be prescribed

2.2. **Establishment**

CERT-In has been operational since January, 2004.

2.3. **Resources**

CERT-In has a team of 95 technical members.

2.4. **Constituency**

The constituency of CERT-In is the Indian cyber community and Indian cyberspace. CERT-In provides services to the organizations in the Government, Public and Private sectors. In addition, CERT-In provides services to the individuals and home users also.

3. Activities & Operations

3.1. **Scope and definitions**

CERT-In provides:

- Proactive services in the nature of Advisories, Security Alerts, Vulnerability Notes, and Security Guidelines to help organisations secure their systems and networks
- Reactive services when security incidents occur so as to minimize damage
- Security Quality management services in the form of cyber security audits, promotion of best practices and cyber security exercises/drills

3.2. **Incident handling reports**

The summary of activities carried out by CERT-In during the year 2018 is given in the following table:

Activities	Year 2018
Security Incidents handled	**208456**
Security Alerts issued	**193**
Advisories Published	**36**
Vulnerability Notes Published	**222**
Trainings Organized	**24**
Indian Website Defacements tracked	**16655**

Table 1: CERT-In Activities during year 2018

3.3. **Abuse statistics**

In the year 2018, CERT-In handled **208456** incidents. The types of incidents handled were Website intrusion & Malware propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements, Unauthorized Scanning activities and Vulnerable Services.

The summary of various types of incidents handled is given below:

Security Incidents	2018
Phishing	**454**
Network Scanning / Probing/Vulnerable Services	**127481**
Virus/ Malicious Code	**61055**
Website Defacements	**16655**
Website Intrusion & Malware Propagation	**905**
Others	**1906**
Total	**208456**

Table 2: Breakup of Security Incidents handled

Various types of incidents handled by CERT-In are given in Figure 1.

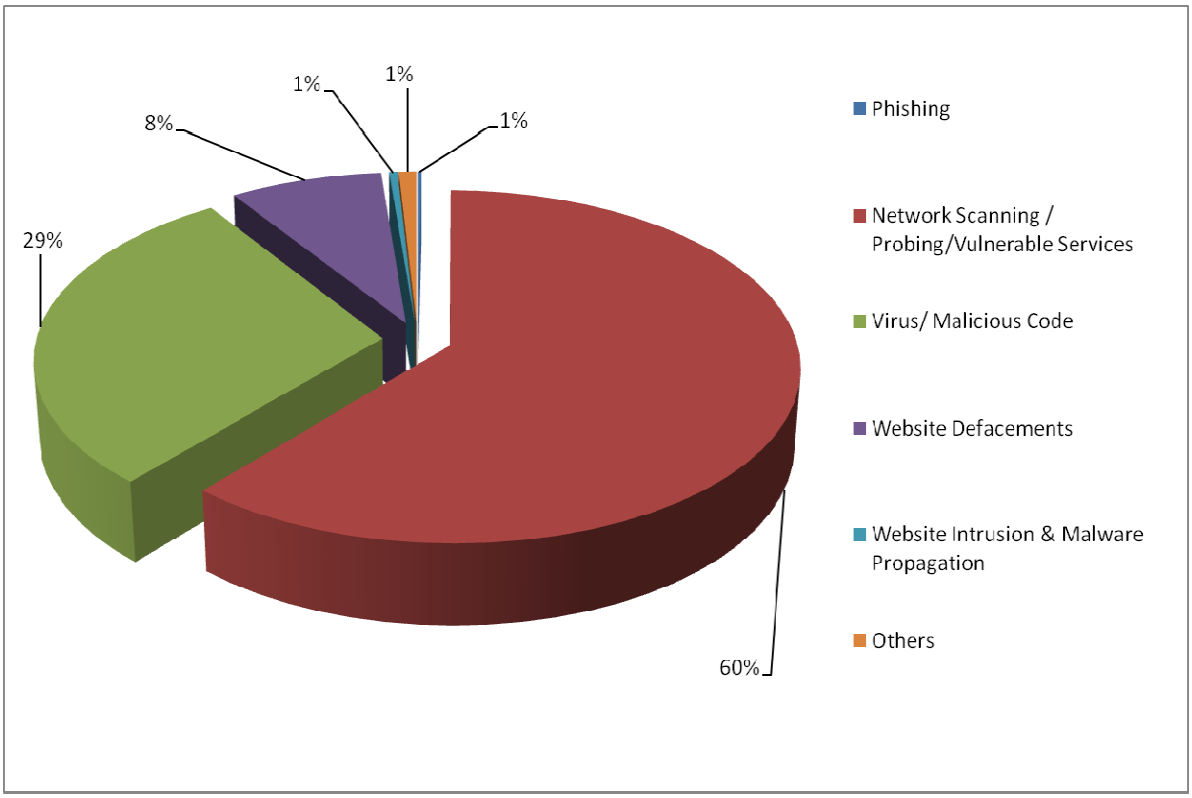

Figure 1: Summary of incidents handled by CERT-In during 2018

3.3.1. **Tracking of Indian Website Defacements**

CERT-In has been tracking the defacements of Indian websites and suggesting suitable measures to harden the web servers to concerned organizations. A total of **16655** numbers of defacements have been tracked.

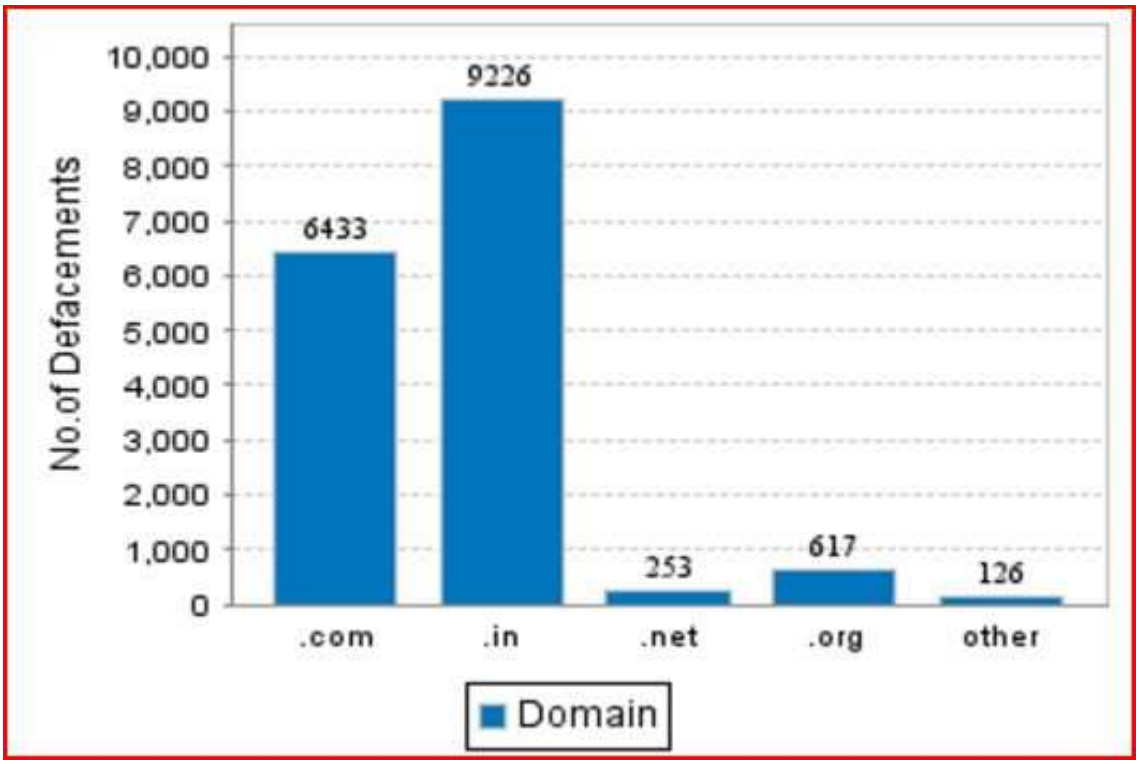

Figure 2: Indian Website Defacements tracked by CERT-In during 2018

3.3.2.Botnet Cleaning Initiatives

Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra - www.cyberswachhtakendra.gov.in) has been established by CERT-In for detection of compromised devices in India and to notify, enable cleaning and securing systems of end users to prevent further malware infections. The centre is working in close coordination and collaboration with Internet Service Providers academia and Industry.

Botnet Cleaning and Malware Analysis Centre ("Cyber Swachhta Kendra") was awarded as one of 51 "Gems of Digital India 2018" in June 2018. "Cyber Swachhta Kendra" also awarded "SKOCH Order-of-Merit and Gold Award" for Cost Effective Cyber Security Model in the month of December 2018.

Botnets events processed by Botnet Cleaning and Malware Analysis centre (Cyber Swachhta Kentra) during 2018.

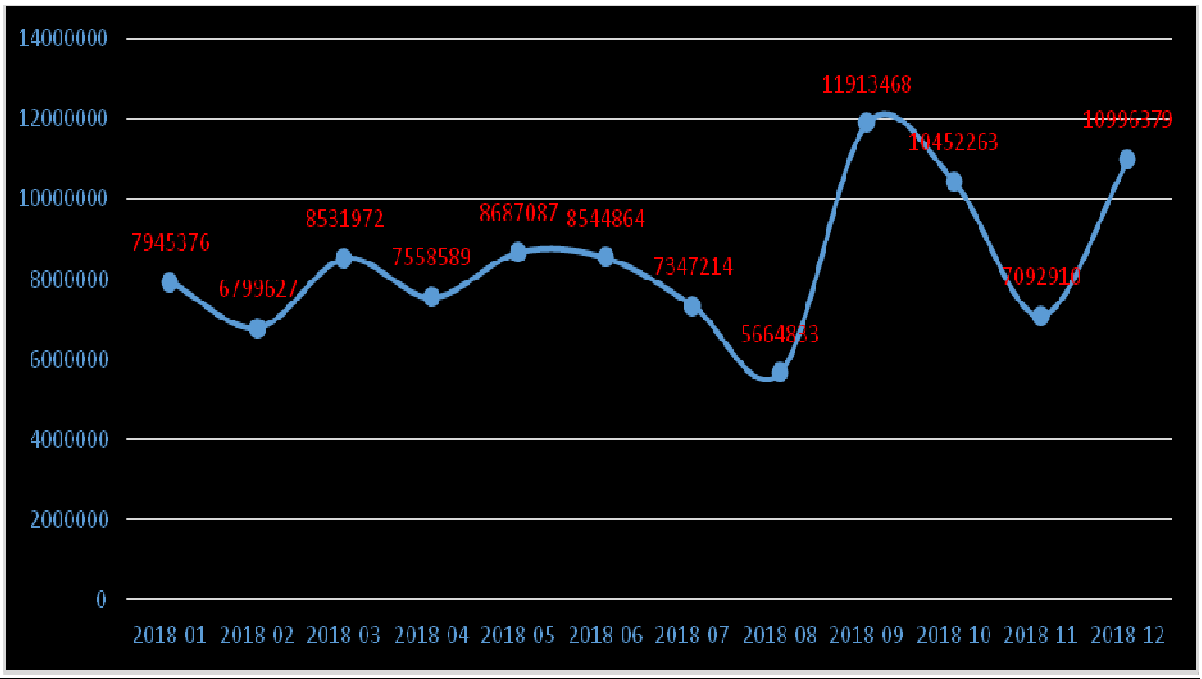

Figure 3: Botnet events tracked by Botnet Cleaning and Malware Analysis Centre

3.3.3. **Security Profiling, Assurance framework and Audit Services**

- Under Security Assurance Framework, CERT-In has empanelled **76** technical IT security auditors to carry out information security audit, including the vulnerability assessment and penetration test of the networked infrastructure of government and critical sector organizations. Government and critical sector organizations are implementing the security best practices in accordance with ISO 27001 standard and as per the advice issued by CERT-In. Services of CERT-In empanelled technical IT security auditors are being used to verify compliance.
- Government and critical sector organizations are implementing the security best practices in accordance with ISO 27001 standard and as per the advice issued by CERT-In. Implementation enabling workshops/interactions have been conducted. Services of CERT-In empanelled technical IT security auditors are being used to verify compliance.
- CERT-In has also carried out episodic security audits of key organizations for enhancing their security posture.

4. Events organized / hosted

4.1. **Security awareness, skill development and training**

In order to create security awareness within the Government, Public and Critical Sector organisations, CERT-In regularly conducts trainings / workshops to train officials of Government, critical sector, public sector industry, financial & banking sector on various contemporary and focused topics of Cyber Security. In 2018, CERT-In has conducted 24 trainings on various specialized topics of cyber security. A total of 746 officers including system/Network Administrators, Database Administrators, Application Developers, IT Managers, Chief Information Security Officers (CISOs)/ Chief information officers (CIOs), and IT Security professional have been trained. CERT-In carried out a specific training session only for women IT professionals.

CERT-In has conducted the following training programmes in 2018:

- Workshop on " Protection Against Social Media Misuse & Cyber Frauds " in January 2018
- Joint Workshop with JPCERT/CC on “Android Security & Secure Coding" at New Delhi in February 2018
- Joint Workshop with JPCERT/CC on "Android Security & Secure Coding” at Bengaluru in February 2018
- Workshop on " Redefining Cyber Security " in February 2018
- Workshop on "Cyber Security Threats & Mitigations" in February 2018
- Workshop on " Darknet and Importance of Cyber Intelligence For Next Gen SoC" in March 2018
- Workshop on "Workshop on Cyber Threats & Countermeasures" in March 2018
- Workshop on "Cyber Crisis Management Plan" in May 2018
- Workshop on " Cyber Threat Hunting with Analytics " in June 2018
- Workshop on " Cyber Crisis Management Plan" in June 2018
- Workshop on “"Combating Advanced Cyber Security Threats using Artificial Intelligence " in July 2018
- Workshop on " Cyber Crisis Management Plan " in August 2018
- Workshop on " SDWAN Security & Next Generation Firewall " in August 2018
- Workshop on "Advanced Cyber Security Threats Detection & Mitigation" in September 2018
- Workshop on "Cyber Threats & Countermeasures" in September 2018
- Workshop on " Cyber Threat Landscape & Role of CERT-In" in September 2018

- Workshop on " Automated Security Configuration Management" in September 2018
- Workshop on " Cyber Threats & Role of CERT-In " in October 2018
- Workshop on " Cyber Threats and Countermeasures exclusively" in October 2018
- Workshop on " Network Security, Visibility & Monitoring " in October 2018
- Workshop on " Workshop on Vigilance Awareness " in October 2018
- Workshop on "Cyber Crisis Management Plan" in November 2018
- Workshop on " Cyber Threat Landscape & Role of CERT-In" in December 2018
- Workshop on " Workshop on Cloud Security" in December 2018

4.2. **Cyber Security Exercises**

Cyber security exercises are being conducted by the Government to help the organizations to assess their preparedness to withstand cyber attacks. These exercises have helped tremendously in improving the cyber security posture of the information infrastructure and training of manpower to handle cyber incidents, besides increasing the cyber security awareness among the key sector organizations. CERT-In has conducted 11 exercises in 2018.

4.3 **Cyber Forensics**

CERT-In is equipped with the tools and equipment to carry out retrieval and analysis of the data extracted from the digital data storage devices using computer forensics and mobile device forensic techniques. CERT-In's facility for Digital Forensics data extraction and analysis is being utilised in investigation of the cases of cyber security incidents, submitted by central and state government ministries, departments, public sector organizations, law enforcement agencies, etc. CERT-In imparts training through workshops organised by CERT-In on computer forensics and mobile device forensics through lectures, demonstrations and hands on practical sessions, which covers seizing, preservation, imaging and analysis of the data retrieved from the digital data storage devices. CERT-In also provides support to the other training institutes in imparting training by delivering lectures with demonstrations on various aspects of cyber forensics.

5. International Collaboration

5.1. **International partnerships and agreements**

Strengthening International cooperation to effectively deal with cyber security issues has been one of the main focus areas of the Government. As such, this aspect is being dealt with

by way of security cooperation arrangements in the form of Memorandum of Understandings (MoUs) between Indian Computer Emergency Response Team and its overseas counterpart agencies that are willing to work together and share information in a timely manner for preventing cyber incidents and cyber attacks as well as collaborating for providing swift response to such incidents. In 2018 CERT-In signed MoUs on cyber security cooperation with two countries namely The Department of Information Communications Technology, The Republic of Seychelles and The Moroccan Computer Emergency Response Team (ma-CERT), National Defence Administration, The Kingdom of Morocco to enable information sharing and collaboration for incident resolution. CERT-In is regularly coordinating with leading service providers and product vendors within and outside the country to obtain advance information on latest cyber threats and attack trends and devise appropriate proactive and preventive measures.

5.2. **Drills & exercises**

CERT-In played the role of EXCON and also participated as a player in APCERT Drill 2018 conducted in March 2018 based on the theme "Data breach via malware on IoT" to test the response capability of leading Computer Security Incident Response Teams (CSIRT) from the Asia Pacific economies. The objective was to enables CERTs to review, practice and strengthen computer security incident handling mechanism and exercise coordination with multiple parties (internal and external) when handling computer security incidents.

CERT-In participated in the ASEAN CERTs Incident Response Drill (ACID) in September 2018 wherein the objective was strengthening cyber security preparedness of ASEAN member states and Dialogue partners in handling cyber incidents and reinforce regional coordination to test incident response capabilities. The theme of the drill was handling System Vulnerabilities and Crypto currency Mining.

CERT-In participated in The Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) drill in September 2018. The theme of the drill was handling Crypto-currencies Risks and Emerging Threats.

5.3. **Other international activities**

- CERT-In participated in Asia Pacific Regional Internet Conference on Operational Technologies (APRICOT) Conference and APCERT SC Meeting from 24 to 28 February 2018 at Kathmandu, Nepal.
- CERT-In participated in the Asia Pacific Computer Emergency Response Teams

(APCERT) Annual General Meeting (AGM), Steering Committee (SC) Meeting and Conference 2018 from 21 to 26 October 2018 at Shanghai, China.

- CERT-In participated in the FIRST AGM & Conference and National CSIRT Meetings from 25 to 30 June 2018 at Kuala Lumpur, Malaysia.
- CERT-In participated in 3rd Singapore International Cyber Week (SICW), Annual Meeting of the Global forum for Cyber Expertise (GFCE) and 6th Europol-INTERPOL Cybercrime Meetings from 18th to 20th September 2018 at Singapore.
- CERT-In was an observer at the NATO "Cooperative Cyber Defense Centre of Excellence" organised Cyber Defense Exercise "Locked Shields 2018". Locked shields is the world's largest and most complex international technical cyber defense exercise.
- CERT-In is a contributing member of review group of the Second Security, Stability, and Resiliency (SSR2) of the Domain Name System(DNS) Review is mandated by Internet Corporation for Assigned Names and Numbers (ICANN) Bylaws Section 4.6(c) to examine how effectively ICANN is meeting its commitment to enhance the operational stability, reliability, resiliency, security and global interoperability of the systems/processes internal/external) that affect the Internet's unique identifiers. The SSRReview Team is reviewing the extent to which ICANN has successfully implemented its security efforts, the effectiveness of the security efforts to deal with actual and potential challenges and threats to the security and stability of the DNS, and the extent to which the security efforts are sufficiently robust to meet future challenges and threats to the security, stability, and resiliency of the DNS, consistent with ICANN's Mission.
- CERT-In has participated in meetings of Internet Governance Forum (IGF) and the discussions under the Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA) has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations in 2018.
- CERT-In is a participating and contributing task force member in the Cyber Incident Management and Critical Information Protection working group of the Global Forum for Cyber Expertise (GFCE), a global platform for countries, international organisation and private companies to exchange best practices and expertise on cyber capacity building by indentifying successful policies, practices and ideas so as to multiply these on a global level.

6. Future Plans

6.1. **Future projects**

CERT-In has evolved as the most trusted referral agency in the area of information security in the country. The future plans envisaged are:

- A full pledged automated Threat Information and Intelligence sharing platform for sharing Indicators of Compromise (IoCs) across stake holders will come up in the coming year.
- A full pledged version of Threat and Situational Awareness Project (TSAP) named National Cyber Coordination Centre (NCCC) will be implemented by CERT-In in the coming years.

6.2. **APCERT Working Groups**

- IoT Security Working Group
    - To ensure the secure usage of IoT devices in priority sectors and build trust in secure usage of IoT Ecosystem

- Secure Digital Payments Working Group
    - Build trust in secure usage of digital payments so as to ensure economic stability.

Contact Information

Postal Address:

Indian Computer Emergency Response Team (CERT-In)
Department of Electronics & information Technology
Ministry of Communication & information technology
Government of India
Electronic Niketan
6, CGO Complex, Lodhi Road
New Delhi – 110003, India

Incident Response Help Desk:

Phone: +91-11-24368572
+91-1800-11-4949 (Toll Free)

Fax: +91-11-24368546

+91-1800-11-6969 (Toll Free)

PGP Key Details:

User ID: incident@cert-in.org.in

Key ID: 0x643B5C9F

Key Type: RSA

Expires: 2019-05-23

Key Size: 4096/4096

Finger Print: 4604 0698 6802 80E4 13E0 091D 4C31 F91E 643B 5C9F

User ID:

info@cert-in.org.in

advisory@cert-in.org.in

subscribe@cert-in.org.in

Key ID: 0xCCA20F32

Key Type: RSA

Expires: 2019-05-23

Key Size: 4096/4096

Finger Print: 9486 28E6 0268 8DD2 47AF DE72 579D 0C18 CCA2 0F32

*****