Programme

Key Note Address
Mrs. Junu Rani Das Kailay, Controller of Certifying Authorities (CCA), MeitY, Government of India


Mrs. Junu Rani Das Kailay

Brief Biodata
Mrs. Junu Rani Das Kailay is the Controller of Certifying Authorities, Government of India since September 2016 and also holding additional charge of Controller of Digital Locker Authority from October 2016. Earlier she had worked for over 30 years in the National Informatics Centre (NIC) and headed various groups. In NIC, she was responsible for major ICT interventions in many sectors such as Finance, Labour & Employment, Health and Education.She was the Managing Director, for 3 years, of National Informatics Centre Services Incorporated (NICSI), a company under Ministry of Electronics & Information Technology for providing and procuring IT solutions for e-governance projects. She also headed National Institute of Electronics & Information Technology (NIELIT) at Chandigarh for 3 years. NIELIT is an Autonomous Scientific Society of Ministry of Electronics & Information Technology involved in Human Resource Development and related activities in the area of Information, Electronics & Communications Technology. She was Vice President (Asia Pacific), Intergovernmental Informatics Programme of UNESCO during 1999-2000. She was responsible for drafting the new programme of UNESCO "Information for all" as a part of four member working group.
Mrs. Kailay holds a Master of Science degree in Physics with specialization in Solid State Physics and a Master of Philosophy degree in Computer Science.

Title of Talk
PKI in Banking Technology


Mr. E. Ravinder

Abstract
Public Key Infrastructure plays an important role in online banking assuring safe financial transactions. In this talk, we shall discuss about the role of IDRBT as a Certification Authority for banks and shall discuss about various PKI enabled banking applications. The talk will be followed up with the present status of applications with opportunities and challenges ahead.

Brief Biodata
Mr. E. Ravinder is Assistant General Manager (Systems) in the Department of Certifying Authority, IDRBT, Hyderabad. He is on deputation from State Bank of India. He has a vast experience of 32 years in Banking and 26 years in Banking Technology. He joined the Bank in the year 1986 and shifted to IT vertical and working in Banking technology since 1992. He holds M.Tech in Computer Science and CAIIB, CISA.

Title of Talk
eSign Services


Ms. Jahnavi Bodhankar

Abstract
e-Sign framework was evolved as part of Government of India's Digital India Initiative. e-Sign is an online electronic signature service, which can be integrated with service delivery applications via an open API to facilitate an e-Sign user to digitally sign a document. Using OTP/Biometric authentication of the Aadhaar holder through Aadhaar e-KYC service, online electronic signature

service is facilitated. e-Sign service facilitates instant signing of documents online by citizens in a legally acceptable form. The services are being leveraged by various applications in Financial Sector, Government agencies for internal office use, Legal Document Signing etc. Various benefits that e-Sign provides include convenience and ease of operations to the signer, streamlined processes and reduction in the costs of operations largely associated with handling and storage of paper.

Brief Biodata
Jahnavi Bodhankar did her M. Sc (Computer Science) from Guru Ghasidas University Bilaspur, M. Tech. (Computer Technology) from NIT Raipur. She is working as Joint Director at C-DAC, Pune where she is associated with projects in the areas of Machine Translation project like MANTRA-Rajbhasha, Anuvadaksh (English to Indian language translation System) and Digital Signatures (e-Hastakshar: C-DAC's On-line Digital Signing Service). She has more than 13 years of experience in Research and Development.

Title of Talk
PKI Technologies

Dr. Mohammed Misbahuddin

Abstract
India is currently riding the wave of digital transformation, and a robust cashless economy is an essential component of it. Assurance about the safeness of a technology is a must for its wide-spread adoption apart from the convenience that it provides. Therefore, in the context of financial institutions, it is important to assure the users about the trust-worthiness of the electronic systems. The technology of Public Key Infrastructure (PKI) along with its widely used atomic application – Digital Signatures is the only globally accepted system for assuring trust-worthy systems. It is therefore essential for all stakeholders to understand how the components of trust – Authenticity, Integrity, Non-repudiation and Confidentiality - are assured through this technology.

Brief Biodata
Dr. Mohammed Misbahuddin did his B.Tech. (CSE) from Gulbarga University, M.Tech. (S/w Engg.) from JNTU-Anantapur and PhD (CSE) in Network Security from JNTU Hyderabad. He is working as Joint Director at C-DAC, Bangalore, where he is associated with projects in the areas of Cyber Security, Digital Signatures PKI and e-Authentication. He is the initiator and Co-Investigator of National e-Authentication Project called “e-Pramaan”. He was instrumental in drafting the e-Authentication Standards for MeitY, Govt. of India. He has more than 16 years of experience in Research, Training and Project Development. He has around 40 Research publications published in International Journals and Conferences. His areas of interest include Information Security, Strong Authentication, PKI, Risk based Engines, DNA Cryptography and DNS Security.

Title of Talk
Post Quantum based Certification Authority

Dr. M. Prem Laxman Das

Abstract
Digital Signature Infrastructures use elliptic curve or RSA based signatures. Quantum computers can run Shor's algorithm, which is polynomial time quantum algorithm for solving factorization and discrete log. We shall discuss signature security in a post-quantum era. We shall also discuss likely candidates which may replace Elliptic Curve Cryptography (ECC) and RSA.

Brief Biodata
Dr. M. Prem Laxman Das is a Senior Scientist at SETS, Chennai. He has completed Ph.D. in Mathematics from Indian Statistical Institute, Kolkata. He works broadly in the domain of algorithmic aspects of Algebra and Number Theory. In Cryptology, his interests include cryptanalysis of public key systems, pairing-based crypto with applications to cloud computing security and aspects of Post Quantum Cryptography (PQC). He is currently executing a project on Security for MANETs funded by BEL.

Title of Talk
PKI Implementation

Mr. Kunal Abhishek

Abstract
Security is one of the biggest concerns especially while communicating over untrusted channels. One of the most efficient solutions of such problem is to use public key infrastructure (PKI) to ensure a reliable, safe and trusted network communication. PKI is a complex subject and still evolving in terms of its utilization in the commercial and e-commerce sectors. Although the underlying technology is quite sound, issues exist in areas such as interoperability and performance. We shall discuss about PKI implementation in this talk.

Brief Biodata
Mr. Kunal Abhishek is a Scientist at SETS, Chennai with 13 years of experience in design and development of Cryptographic and Network Security products/solutions. He also served as Software Engineer in Weapons & Electronic Systems Engineering Establishment (WESEE), an R&D unit of Indian Navy for 7 years. He is Principal Investigator of SETS in-house developed PKI solution called e-Abhedya. He was instrumental in framing "Digital Signature End Entity Rules, 2015" with inclusion of ECC for PKI services under the IT Act of India. His research interest includes ECC based PKI and Secure Kernel Development. He holds an M.S. degree from BITS, Pilani and currently pursuing Ph.D. in Computer Science from Bharathidasan University, Trichy.

Title of Talk
A Note on OpenSSL Library

Mr. T. Santhosh Kumar

Abstract
Digital certificates are an integral part of a Public Key Infrastructure which binds user identity with the certificate and used for authentication, encryption, maintaining integrity and non-repudiation purposes to communicate over untrusted channels. OpenSSL is a popular library used for generating digital certificates and facilitating SSL functionalities. We shall have a quick note on how OpenSSL library can be used for key pair and certificate signing request (CSR) generation and digital certificate generation. We shall also discuss how OpenSSL library can be used for creation of certificate revocation list (CRL).

Brief Biodata
Mr. T. Santhosh Kumar holds B.Tech and M.Tech degrees in Computer Science and Engineering from Bharathidasan University. He is one of the key members of development team of "e-Abhedya" PKI solution at SETS. His research interest includes securing E-mail system and PKI. He is also a RedHat Certified Engineer. He is currently executing a project on Proprietary ECC based PKI funded by BEL at SETS.