Expert Talk
Department of Computer Science and Engineering
Indian Institute of Technology Kanpur
Date: Friday 17 March 2017
Time: 5 pm
Venue: RM 101

ESign: Digital Signature combined with power of online authentication

Rajat Moona
Director General,
C-DAC
moona@cdac.in

Abstract

Digital signatures provide a non-repudiation mechanism for documents or messages. The digital signature are used to validate the integrity of the documents or messages to protect them against tampering as well as to establish the authenticity and to provide genuineness. In order to establish the non-repudiation, digital signature mechanism is backed up by a complex certifying authority (CA) mechanism to certify the individual signers so that their public key can be used with trust on the CA to verify the digital signatures. This mechanism however requires the issuance of digital signature certificates, verification of the individual's credentials and the legal support for digital signatures. Often the verification of the credentials involve physical means for the verification, as is usually demanded by law. India provides a unique proposition of Aadhaar, where the residents of the country are provided a unique online-verifiable identity after credential verifications, registration of fingerprint and iris biometric. Aadhaar provides a service of authentication as well as "know-your-customer" through online authorization by the identified individual. These services are provided by Aadhaar through a network of Aadhaar-authorized agencies.

Esign integrates the powerful Aadhaar authentication service with certification authority services and provides one-time use certificates along with digital signatures on the documents provided by an individual. This mechanism therefore provide an instant method of obtaining a variety of e-governance services which are tenable under the applicable laws and provide non-repudiation. In this talk, we discuss the mechanism of ESign, its powerful features and domains where such technology can be effectively used. We also discuss implementation and issues related to the implementation and techniques to overcome them.

Speaker Bio: Prof. Moona heads the Centre for Development of Advanced Computing (C-DAC) in capacity of Director General and leads C-DAC's initiatives in the areas of High Performance Computing, Multilingual Computing, Professional Electronics, Cyber Security, Health Informatics, e-Governance, Education and Training. Prof. Moona is also a Professor of Computer Science at IIT Kanpur and has supervised several postgraduate theses. He along with his students and colleagues, has authored 10 patents, several research papers and books.
He had been instrumental in defining applications such as smart card driving licence, vehicle registration, e-passport, electronic toll collection, mobility card, etc. The research area of Prof. Rajat Moona spans over embedded computing, computer security, VLSI design and Operating Systems. In the past Prof. Moona had been a visiting Scientist to MIT and a senior Engineering Manager at Mentor Graphics. Prof. Moona is recipient of several awards and recognitions, including Indo-US Science and Technology Fellowship, Poonam and Prabhu Goel Chair Professorship, VASVIK Award for the year 2010, IESA Techno Visionary Award 2014, fellowship of Maharashtra Academy of Sciences 2015 and on National Voters Day in January 2017, Prof. Moona received an award from the Hon'ble President of India, Shri Pranab Mukherjee for his role as member of Technical Expert Committee for Election Commission of India. Prof. Moona is Director Designate, IIT Bhilai-Durg and is likely to take up the new position soon.