R F D

RESULTS-FRAMEWORK DOCUMENT

for

Controller of Certifying Authorities

Department of Information Technology

(2011-2012)

SECTION 1:

Vision, Mission, Objectives and Functions

Vision

- To create Trust in Electronic Transactions.

Mission

- Authentication of transactions performed in the Electronic environment.

Objectives

- Implementation of authentication system in electronic environment through Public Key Infrastructure (PKI)
- To create awareness about the authentication techniques in the PKI.

Functions.

- Exercising supervision over the activities of the Certifying Authorities;
- Certifying public keys of the Certifying Authorities
- Laying down the standards to be maintained by the Certifying Authorities;
- Specifying the qualifications and experience which employees of the Certifying Authorities should possess;
- Specifying the conditions subject to which the Certifying Authorities shall conduct their business;

- Specifying the content of written, printed or visual material and advertisements that may be distributed or used in respect of a Electronic Signature Certificate and the Public Key;
- Specifying the form and content of a Electronic Signature Certificate and the key;
- Specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
- Specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
- Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
- Specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
- Resolving any conflict of interests between the Certifying Authorities and the subscribers;
- Laying down the duties of the Certifying Authorities;
- Maintaining a data-base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

SECTION 2: *Inter se* Priorities among Key Objectives, Success indicators and Targets

(1st April 2011 – 31st March 2012)

Column 1	Column 2	Column 3	Column 4		Column 5	Column 6				
Objective	Weight	Actions	Success Indicator	Unit	Weight	Target / Criteria Value				
						Excellent	Very Good	Good	Fair	Poor
						100%	90%	80%	70%	60%
Objective 1 • Implementation of authentication system in electronic environment through Public	70	**Action 1** Auditing of Certifying Authorities	Number of Certifying Authorities audited	Number	20	7	6	5	4	2

Key Infrastructure (PKI).		**Action 2** Certifying the Public Keys of the Certifying Authorities and Publishing of the Certificate.	Average Time taken for Publishing of the Certificates on CCA's Website.	Days	10	20	22	25	28	30
		Action 3 Publishing the Certificate Revocation List (CRL) of certifying Authorities.	Average Time taken for publishing of CRL from the due date.	Days	10	33	34	35	36	37
		Action 4 Issuance/Renewal of Licences	Average Time taken for Issuance of the Licences to the new applicant or Renewal of Licences of the Existing CA's after receiving the complete Application.	Days	15	50	53	55	58	60

		Action 5 Up-gradation of standards to change the Hashing Algorithm from SHA -1 to SHA-2	Completion of implementation of Hashing Algorithm to SHA-2	Date	15	10th March 2012	15th March 2012	20th March 2012	25th March 2012	31th March 2012
Objective 2 • To create awareness about the authentication techniques in the PKI.	19	**Action 1** To Facilitate the awareness programmes on Digital Signature/IT Laws in various organisations.	Awareness Programmes Facilitated.	Number	19	14	12	10	8	6

Mandatory Success Indicators

Each RFD must contain the following mandatory indicators to promote enhanced and sustainable organisational performance levels.

Objective	Actions	Success Indicator Unit	Unit	Weight	Excellent 100%	Target Very Good 90%	Criteria Good 80%	Value Fair 70%	Poor 60%
Efficient Functioning of the RFD System	Timely submission of RFD for 2011-12	On-time submission	Date	2%	March 31 2011	April 3 2011	April 4 2011	April 5 2011	April 6 2011
	Timely submission of Results for 2011-12	On-time submission	Date	1%	May 1 2012	May 3 2012	May 4 2012	May 5 2012	May 6 2012
	Finalize a Strategic Plan for RC	Finalize the Strategic Plan for next 5 years	Date	2%	Dec. 10 2011	Dec. 15 2011	Dec. 20 2011	Dec. 24 2011	Dec. 31 2011
	Identify potential areas of corruption related to organization activities and develop an action plan to mitigate them	Finalize an action plan to mitigate potential areas of corruption.	%	2%	Dec. 10 2011	Dec. 15 2011	Dec. 20 2011	Dec. 24 2011	Dec. 31 2011

	Implementation of Sevottam	Create a Sevottam complaint system to implement, monitor and review Citizen's Charter	Date	2%	Dec. 10 2011	Dec. 15 2011	Dec. 20 2011	Dec. 24 2011	Dec. 31 2011
		Create a Sevottam Complaint system to redress and monitor public Grievances	Date	2%	Dec. 10 2011	Dec. 15 2011	Dec. 20 2011	Dec. 24 2011	Dec. 31 2011
		TOTAL WEIGHT	=	11%					

SECTION 3: Trend Values of the Success Indicators

Column 1	**Column 2**	**Column 3*mn 3***	**Column 4**		**Column 5**	**Column 6**	**Column 7**	**Column 8**	**Column 9**
Objective	Weight	***Actions***	Success Indicator	Unit	Actual Value for FY 09-10	Actual Value for FY 10-11	Target Value for FY 11-12	Projected Value for FY 12-13	Projected Value for FY 13-14
Objective 1 • Implementation of authentication system in electronic environment through Public Key	70	**Action 1** Auditing of Certifying Authorities	Number of Certifying Authorities audited	Number	7	7	6	7	7

Infrastructure (PKI).		**Action 2** Certifying the Public Keys of the Certifying Authorities and Publishing of the Certificate.	Average Time taken for Publishing of the Certificates on CCA's Website.	Days	24	23	22	20	19
		Action 3 Publishing the Certificate Revocation List (CRL) of certifying Authorities.	Average Time taken for publishing of CRL from the due date.	Days	36	35	34	33	32
		Action 4 Issuance/Renewal of Licences	Average Time taken for Issuance of the Licences to the new applicant or Renewal of Licences of the Existing CA's after receiving the complete Application.	Days	58	55	53	52	50

		Action 5 Up-gradation of standards to change the Hashing Algorithm from SHA -1 to SHA-2	Completion of implementation of Hashing Algorithm to SHA-2	Date	-	-	15th March 2012	-	-
Objective 2 • To create awareness about the authentication techniques in the PKI.	19	**Action 1** To Facilitate the awareness programmes on Digital Signature/IT Laws in various organisations.	Awareness Programmes Facilitated.	Number	13	15	12	13	14

SECTION 4: Description and Definition of Success Indicators and Proposed Measurement Methodology

Success indicators	Description and definition	Measurement methodology
Number of Certifying Authorities audited	The physical and technical infrastructure audit of Certifying Authorities is undertaken to check the compliance with the provisions of the Information Technology Act, 2000, Rules, Regulations and Guidelines issued under it.	Number of Certifying Authorities audited.
Average Time taken for Publishing of the Certificates on CCA's Website.	The Public Key of the Certifying Authorities is Certified by CCA as per provisions of the Information Technology Act, 2000.Request for such Certification are received from the Certifying authorities on start of their operations as well as during the course of time in case of change in any of the field in the Certificate. The Public Key Certificate of the Certifying Authorities is Published on CCA's Website for Authentication and Verification Purposes.	Average Time taken for Publishing the Public Key Certificate.
Average Time taken for publishing of CRL from the due date.	The Certificate Revocation List of the Revoked Certificate is Published on the CCA's Website. The CRL is published before the last date of the Validity period of the current CRL or in between also whenever there is a Certificate Revocation request from the Certifying Authority. The relaying parties check the status of the Certificate before the Verification.	Average Time taken for Publishing the CRL.

Average Time taken for Issuance of the Licences to the new applicant or Renewal of Licences of the Existing CA's after receiving the complete Application.	The Licence to the Certifying Authority is Granted as per the provisions of the Information Technology Act, 2000, Rules, Regulations and Guidelines issued under it. Any individual/Firms/Company can make a request for grant of Licence on fulfilment of various conditions/requirements as per the Information Technology Act, 2000. Renewal of the licence needs to be granted on request to the existing Licensed Certifying Authorities as per the Information Technology Act, 2000.	Average Time taken for Granting the new licence /Renewal of the licence.
Completion of implementation of Hashing Algorithm to SHA-2	Currently, Hashing Algorithm SHA-1 (160 Bits) is used for creation of Digital Signatures by Subscribers. Stronger Hashing Algorithm SHA-2 (256 Bits) is required for providing improved security against various attacks.	Date of completion of implementation of Hashing Algorithm SHA-2.
Awareness Programmes Facilitated.	Various Organisations conduct awareness programmes for users, police, judicial officers and other Government officers to create awareness about the Digital Signatures, use of technology and the associated legal aspects. Organisations are Facilitated by providing resources which include technical Support by way of providing Speakers/ Course content and/or Financial supports by providing requisite funds.	Number of awareness programmes Facilitated.

SECTION 5:

Specific Performance Requirements from other Departments

Departments	Relevant Success Indicator	What do you need?	Why do you need it?	How much you need?	What happens if you do not get it?
—	—	—	—	—	—

SECTION 6:

Outcome / Impact of activities of organisation ministry

1	2	3	4	5	6	7	8	9
S. No	Outcome / Impact of organisation / RCs	Jointly Responsible for influencing this Outcome / Impact with the following organisation(s) /departments/ministry(ies)	Success Indicator(s)	2009-2010	2010-2011	2011-2012	2012-2013	2013-2014
1	Implementation of PKI based authentication system to create trust in electronic transactions.	CCA / Certifying Authorities.	Number of Signatures issued in Lakhs.	3.9 Lakhs	5.4 Lakhs	6.0 Lakhs	7.0 Lakhs	8.0 Lakhs