Minutes of the Dohatec CA

Key Generation Ceremony

Date: July 3, 2012

Version:1.0

Author: DohatecCA

Revised by: Participants

Approved by: Participants

Document Classification: Public

Reference No:Key_Ceremony_Minutes July 3 2012.docx

HGSGh LS Jinat Rehana SH

Document History

Version	Date	Comments	Modified Pages	Page No
V-1.0	July 3, 2012			

This Document is intended for use only by Dohatec Certifying Authority.

Hasan LS Jinat Rahman

Minutes of the Dohatec CA Key Generation Ceremony

Date: 3 July 2012

Venue: On July 3, 2012 the Key Generation Ceremony for Dohatec CA started at 11:00 AM with Pre-key Ceremony Briefing Meeting in the meeting room of Conference Building of Dohatec New Media at 44/1, Purana Paltan Line, Dhaka-1000, attended by the officials from CCA Bangladesh, along with the external Auditor and personnel of Dohatec CA. The Dohatec CA is located at Doha House, 43, Purana Paltan Line, Dhaka.

Attendees

Following participants attended the Dohatec CA Key Generation Ceremony:

Luna Shamsuddoha, Chairman, Dohatec New Media

AKM Shamsuddoha, Proprietor and President, Dohatec New Media

Nazmul Huda, CEO, Dohatec New Media

FahmidaAkter, Dohatec CA Certifying Authority Administrator I (CAA- I)

Jinat Rehana, Dohatec CA Certifying Authority Administrator II (CAA-II)

Md. Masudur Rahaman, Dohatec CA Registration Authority Administrator (RAA)

Masudul Haque, Dohatec CA System Administrator (SA)

Dewan Samsul Huda, Dohatec CA Database Administrator (DBA)

Mustafizul Haque, Dohatec CA Network Administrator (NA)

The Ceremony was recorded and photographed by the following persons.

Harunur Rashid, Videographer

Shanjir Hossain, Photographer

Hossain LS Jinat Rehana SH

Roles of Trusted Attendees

During the Ceremony the following attendees are appointed to the trusted roles of Dohatec CA

Luna Shamsuddoha, Chairman, Dohatec New Media as:

- Key Ceremony Administrator
- Dohatec CA Data Safe Key Holder
- Dohatec CA Document Safe Key Holder
- Dohatec CA Data Center Access Key Holder

Fahmida Akter, Dohatec CA CAA -I as:

- Dohatec CA CAA-I
- Black Token Holder1
- Black Token PIN Code1 Holder

Jinat Rehana, Dohatec CA CAA -II as:

- Support for Key Ceremony Administrator

Md. Masudur Rahaman, Dohatec CA RAA as:

- RAA
- Black Token Holder2
- Black Token PIN Code2 Holder

Masudul Haque, Dohatec CA SA as:

- Dohatec CA SA
- HSM PED Holder
- RED Token Holder
- RED Token PIN Code Holder
- Blue Token Holder
- Blue Token Password Holder

Dewan Samsul Huda, Dohatec CA DBA as:

- Support for Dohatec CA SA

Hasan LS JinatRehana SH

External Witnesses

SL No	Full Name	Designation	Organization
1.	**Mr. Md. Zahangir Alam (ndc)**	Controller of Certifying Authorities Controller (Joint Secretary)	Office of the Controller of Certifying Authorities (CCA), Bangladesh
2.	**Mr. AKM Shahabuddin**	Deputy Controller of Certifying Authorities (Admin & Finance)	Office of Controller of Certifying Authorities (CCA), Bangladesh
3.	**Mr. Ziauddin Ahmed**	Assistant Controller (IT Security)	Office of Controller of Certifying Authorities (CCA), Bangladesh
4.	**Mr. Md. Hasan-uj-Zaman**	Assistant Programmer	Bangladesh Computer Council .
5.	**Mr. Mohammad Tohidur Rahman Bhuiyan**	External Auditor	CEO & Lead Auditor RightTime Limited
6.	**MD. Badrul Alam**	Advocate and Notary Public	Bangladesh Supreme Court, High Court Division

LS Jinat Alam

Policy References

Dohatec CA Key Generation Ceremony was performed in compliance with Digital Certificate Interoperability Guideline published by Controller of Certifying Authority (CCA), Bangladesh, Dohatec CA Certificate Practice Statement (CPS), other associated policies and procedures for Dohatec CA. Dohatec CA Key Generation Ceremony established that all the associated procedures were followed and implemented.

Declared Pre Installation Tasks

At the onset of the ceremony, the Key Ceremony pre-installation tasks had been declared as follows:

1. Installation of Operating System, Hardening and Antivirus
2. Installation of MS SQL SERVER 2008R2 clustering database on SAN
3. Configuration of Domain Name Server (DNS)
4. Installation of HSM Driver
5. Installation of Cryptographic Operation Control Software(Dhruvam-Lite) on Certificate Generation Machine (CGM).
6. Pre Ceremony Configuration and Preparation

Pre Briefing of the Ceremony

Pre Briefing of the Dohatec CA Key Generation Ceremony started on 11:00 A.M. All Attendees and External Witnesses met at Dohatec New Media premises at Doha House, 43 and 44/1 Purana Paltan Line, Dhaka-1000.The Entry/Exit log for Pre Briefing Session was accessible to all the participants. The Key Ceremony Administrator explained the PKI, the Key Generation Ceremony of Dohatec CAand features and services of Dohatec CAto the participants. The whole Pre Briefing session has been video recorded. At the end of the Pre Briefing Session, all the participants signed off in the Entry/Exit log of the Pre Briefing Session.

Hassan LS Sinat Rehana

The Ceremony was suspended for Tea-break from 11:30AM to 12:00 PM.

Initial Preparation of the Ceremony:

External Witnesses and other Participants were escorted to the 1st Floor of Doha House, 43PuranaPaltan Line, Dhaka-1000by the Key Ceremony Administrator, CAA and attendeesfor witnessing the Ceremony at 12:00PM. The following steps were performed in order to complete the whole Key Generation Ceremony:

1. All the participants sign in the Entry/Exit log of the Technical Session1 of the Ceremony.
2. All the participants accessed the Dohatec Data Centeras follows:
   a. The Key Ceremony Administratorentered the Strong Room by accessing through the Access Control Authentication System at the entrance doors. The Key Ceremony Administrator carried with her the associated documents for performing the ceremony and the key of the Dohatec CA Data Safe.

   b. The Video Recording Specialist entered the Strong Room escorted by the CAA and started video recording of all the activities performed.

   c. All other allowed participants entered the Strong Room one by one and escorted as required by gaining access through the Access Control Authentication System at the entrance doors.
3. The Key Ceremony Administrator made sure that all the participants were present and in their respective locations.
4. The Key Ceremony Administrator introduced all the participants and gave a brief introduction of the Ceremony covering the features of the Strong Room and how the Ceremony was going to be executed.
5. The Key Ceremony Administrator placed the HSM component's Holder terms and declaration forms, and corresponding PIN paper sheets with the envelops on the Inventory Table.

Hasan LS Jinat Rahman

6. The Key Ceremony Administrator unlocked the Dohatec CA Data Safe and brought out 2 HSM PEDs, 3 HSM Red Tokens, 3 HSM Blue Tokens and 3 HSM Black Tokens from the Dohatec CA Data Safe. The Key Ceremony Administrator made the entries in the Log of the Dohatec CA Data Safe recording the reason for bringing out the HSM components from the Data Safe.The HSM components were placed on the inventory table with their corresponding Holder terms and declaration forms and PIN paper sheets.
7. The Key Ceremony Administrator locked the Dohatec CA Data Safe. One of the Internal Witnesses verified that the Data Safe was locked.
8. Dohatec CA SA received the HSM PED and filled up the PED Holder terms and declaration form by carefully reading that. The HSM PED Holder terms and declaration form was kept on the Inventory Table as before.
9. Dohatec CA SA received the PIN paper sheets for HSM Blue Token1, HSM Blue Token2 and HSM Blue Token3. He secretly decided the PIN code by carefully reading the PIN Code generation instruction and entered the same PIN code in the PIN paper sheets for those 3 HSM Blue Tokens. The PIN paper sheets were then put into the corresponding envelops and kept unsealed on the Inventory Table.
10. Dohatec CA SA received the HSM Blue Token1, HSM Blue Token2 and HSM Blue Token 3and filled upthe Holder terms and Declaration formsby carefully reading those.The Blue Token Holder terms and declaration forms were kept on the Inventory Table as before.
11. Dohatec CA SA received the HSM Red Token1, HSM Red Token2 and HSM Red Token3 and filled up the Holder terms and Declaration formsby carefully reading those.The Red Token Holder terms and declaration forms were kept on the Inventory Tableas before.
12. Dohatec CA SA received the Key Ceremony Technical Script from the Key Ceremony Administrator.

Hasan LS Jinat Rahman

13. Dohatec CA CAA-I received the PIN paper sheets for HSM Black Token1, HSM Black Token2 and HSM Black Token3 and secretly decided the PIN code1by carefully reading the PIN Code generation instruction. He entered the same PIN code in the PIN paper sheets for those 3 HSM Black Tokens. The PIN paper sheets were then put into the corresponding envelops and kept unsealedon the Inventory Table.
14. Dohatec CA CAA-I received the HSM Black Token1, HSM Black Token2 and HSM Black Token3.He filled up the Holder terms and Declaration forms as a Holder1 of HSM Black Tokens.The Black Token Holder1 terms and declaration forms were kept on the Inventory Tableas before.
15. Dohatec CA RAA received the PIN paper sheets for HSM Black Token1, HSM Black Token2 and HSM Black Token3and secretly decided the PIN code2by carefully reading the PIN Code generation instruction. He entered the same PIN code in the PIN paper sheets for those 3 HSM Black Tokens. The PIN paper sheets were then put into the corresponding envelops and kept unsealedon the Inventory Table.
16. Dohatec CA RAA filled up the Holder terms and Declaration forms for HSM Black Token1, HSM Black Token2 and HSM Black Token3as a Holder2 of thosetokens.TheBlack Token Holder2 terms and declaration forms were kept on the inventory table as before.
17. Thereafter the Initialization event was commenced.

Initialization Event:

Initialization event started at 12.15PM.

18. Dohatec CA SA powers on the CGM server, DNS and Database Server.

Hasan LS Jinat Rahman

HSM Initialization:

19. Dohatec CA SA Connected the HSM PED to the HSM device using a cableSO Key
20. SO/Admin Key (Blue Token Key) Creation:

    a. Dohatec CA SA inserted the blank HSM Blue Token1 into the USB connector at the top of the HSM PED for creating SO/Admin account.

    b. In the terminal window, Dohatec CA SAaccessed to the HSM(Luna PCI)directory and entered the command to start the lunacm utility.

    c. Dohatec CA SA entered the command giving a label and domain name for initializing the Luna PCI HSM.

    Dohatec CA SA was prompted to continue the initialization process. Dohatec CA SA continued the initialization.

    d. Dohatec CA SA was prompted to attend the HSM PED. Dohatec CA SA chose the option for creating the SO Key with a new SO authentication.

    e. Dohatec CA SA was prompted for entering PIN code for SO Key. Dohatec CA SA entered the PIN code (SO Key) for HSM Blue Token remembering it.

    f. Dohatec CA SA entered the PIN code (SO/Admin Key) again to confirm the Key.

    g. Dohatec CA SA backed up the SO/Admin Key to HSM Blue Token2 and HSM Blue Token3.

21. Domain Key (RedToken Key) Creation:

    a. HSM PED prompted to enter the SO PIN Code and Dohatec CA SA entered the SO PIN Code. Within this step a Domain Key wasgenerated.

    b. HSM PED prompted to insert a blank Token for Domain Key. Dohatec CA SA inserted the HSM Red Token1 into the USB connector at the top of the HSM PED.

    c. Dohatec CA SA backed up the Domain Key to HSM Red Token2 and HSM Red Token3.

22. Dohatec CA SA entered the command in the terminal window in order to verify that the HSM is in FIPS-2 approved operation mode.
23. Dohatec CA SA entered the command to logout from HSM.

Hasan LS Jirat Rahman SH

HSM Partition Creation for Dohatec CA and Black Token Creation:

24. Dohatec CA SA entered the login command in order to login as a Security Officer (SO). He was then directed to the HSM PED.
25. Dohatec CA SA Authenticated himself as SO by inserting the HSM Blue Token1 and entering the SO/Admin PIN.
26. Dohatec CA CAA-I inserted the blank Black Token1 into the USB connector at the top of the PED.
27. Dohatec CA SA entered the command for HSM partition creation in the terminal window. He was then directed to the HSM PED.
28. HSM Access Key (Black Token Key)Creation:
    a. Dohatec CA SA chose the option for creating the HSM Access Key (Black Token Key).
    b. The HSM PED then prompted to enter the PIN code for HSM Access Key. The HSM Access Key is a combination of PIN Code1 and PIN Code 2. Dohatec CA CAA-I entered the HSM Access PIN code1 for HSM Black Token remembering it.
    c. Dohatec CA RAAentered the HSM Access PIN cod2 for HSM Black Token remembering it.
    d. Dohatec CA CAA-I and Dohatec CA RAA entered HSM Access PIN code1and HSM Access PIN code2 one by one again to confirm the Key.
29. Dohatec CA SA entered the command in the terminal window to logout from HSM.
30. Dohatec CA SA handed over the backup HSM Tokens (Blue Token2, Blue Token3, Red Token2, Red Token3, Black Token2 and Black Token3)to the Key Ceremony Administrator.
31. Key Ceremony Administrator kept the token on the inventory table.

Hasan .LS Jinat Rehana

Key Generation Event:

Key Generation Event started at 12:30 PM

32. Dohatec CA SAentered the login command in the terminal window in order to login as a User. He was then directed to the HSM PED.
33. HSM PED prompted to enter user password. Dohatec CAA-I inserted the Black Token1 into the USB connector at the top of the PED and entered HSM Access PIN Code1.
34. Dohatec CA RAA entered HSM Access PIN Code2.
35. Dohatec CA SA entered the command in order to check that the HSM is empty.
36. Dohatec CA SA entered the command for logout and opened another terminal window.

Key Pair Generation:

37. Dohatec CA SA entered the command to run the Cryptographic Operation Control Application(Dhruvam Lite).
38. Dohatec CA SA opened IE browser and entered the URL for accessing the Dhruvam-Lite Application. The Home Page for Dhruvam Lite appeared.

Certificate Signing Request (CSR) Generation:

39. Dohatec CAA-I clicked offline CGM then CGM screen appeared.
40. Dohatec CAA-I clicked CA/Sub-CA -> Generate CA/Sub-CA request.
41. Dohatec CAA-I filled all the required details.
42. Dohatec CAA-I Clicked the submit button.
43. The screen prompted to enter the first Password and second Password of HSM.
44. Dohatec CAA-I inserted the Black Token1 into the USB connector at the top of the PED and entered HSM Access PIN Code1.
45. Dohatec RAA entered HSM Access PIN Code2.
46. After that a Request ID of the Generated CSR was displayed.

Hasan LS Jinat Rehana SH

Download the request from Dhruvam®–Lite:

47. Dohatec CAA-I clicked the Home page.
48. Dohatec CAA-I clicked offline CGM.
49. Dohatec CAA-I clickedDownloads→ Download Request/Certificate.
50. Dohatec CAA-I entered the Request ID field there.
51. Dohatec CAA-I selected the Source as 'Offline'.
52. Dohatec CAA-I selected Format as PEM.
53. Dohatec CAA-I clicked Request and Save to a preferred location.

Checking the HSM:

54. Dohatec CA SA opened a new terminal andentered the login command in order to login as a User. He was then directed to the HSM PED.
55. HSM PED prompted to enter user password. Dohatec CAA-I inserted the Black Token1 into the USB connector at the top of the PED and entered HSM Access PIN Code1.
56. Dohatec CA RAA entered HSM Access PIN Code2.
57. Dohatec CA SA entered the command in order to check that key pair has been created and stored in the HSM.
58. Dohatec CA SA entered the command to take the backup of the generated key pair in a specific location with a preferred file name.

CSR Backup on CD:

59. Dohatec CA SA collected the blank CDs for CSR backup from the Key Ceremony Administrator
60. Dohatec CA SA went to the saved location of the CSR.
61. Dohatec CA SA backed up the CSR on 4 different CDs.
62. Dohatec CA SA handed over the backup CDs to the Key Ceremony Administrator. The Key Ceremony Administrator put the CDs in the corresponding envelops and kept those on the inventory table.

Hasan LS Jinat Rahman

Dohatec CA Key Pair Backup on CD:

63. Dohatec CA SA collected the blank CDs for Dohatec CA key pair backup from the Key Ceremony Administrator
64. Dohatec CA SA went to the saved location of the Dohatec CA key pair.
65. Dohatec CA SA backed up the Dohatec CA key pair on 3 different CDs.
66. Dohatec CA SA handed over the backup CDs to the Key Ceremony Administrator. The Key Ceremony Administrator put the CDs in the corresponding envelops and kept those on the inventory table.
67. Dohatec CA SA handed over the HSM PED, Blue Token1 and Red Token1 to the Key Ceremony Administrator. Dohatec CA CAA-I handed over the HSM Black Token1 to the Key Ceremony Administrator.
68. The Key Ceremony Administrator sealed and signed all the PIN paper sheets.The Key Ceremony Administrator kept all the PIN paper sheets with the corresponding components in the Data Safe. The Key Ceremony Administrator made sure that all the handed over component are kept in the Data Safe.
69. The Key Ceremony Administrator locked the Data Safe and one of the attendees verified that it was locked properly.

The Key Ceremony was stopped at 13:35 PM for lunch and prayer.

All participants of the Ceremony checked-out the operation area signing off in the Entry/Exit log for Technical Session1 that remained guarded for the time of the lunch break.

At 15.10 PM all participants to the Ceremony checked-in the operation area signing in the Entry/Exit log for Technical Session2 and the Ceremony was resumed at 15:10 PM.

Hasan Jinat Rehana

Distribution Event:

Distribution Event started at 15:10 PM

The Key Ceremony Administrator collected the signatures from all the external witnesses and attendees of the ceremonyon the Minutes of the Dohatec CA Key Generation Ceremony.

The Key Ceremony Administrator Collected the Component Holder terms and declaration forms and directed the Notary Public to attest the Forms.

Conclusion:

The Key Ceremony Administrator collected all the signed documents, filed the documents, sealed and kept in an archive Folder.Before any participant left the operation area, the Key Ceremony Administrator made sure that all the components, CDS and video recordings were kept in the Data Safe recording the entries in the Data Safe Log. The Key Ceremony Administrator locked the Data Safe and one of the Attendees verified that the Data Safe was properly locked. All the External Witnesses and Attendees signed off in the Entry/Exit log of the Technical Session2.

The Key Ceremony Concluded at 15:30 PM.

LS Sinat Rahman

List of Signatories

SL No	Full Name	Signature and Date
1	Mr. Md. Zahangir Alam (ndc)	03/7/2012
2	Mr. AKM Shahabuddin	03/7/2012
3	Mr. Ziauddin Ahmed	03/07/12
4	Mr. Md. Hasan-uj-Zaman	Hasan 03/07/2012
5	Mr. Mohammad Tohidur Rahman Bhuiyan	
6	Md. Badrul Alam	
7	Luna Shamsuddoha	Luna Shamsuddoha 3.7.2012
8	Fahmida Akter	
9	Jinat Rehana	Jinat Rehana
10	Md. Masudur Rahman	M. Rahman / M. R
11	Masudul Haque	Masudul Haque 03/07/2012
12	Dewan Samsul Huda	Dewan Samsul Huda