MANGO
TELESERVICES

Mango Teleservices limited

# Mango Root Key Generation Ceremony (2013) Meeting Minutes

11/28/2013

| | |
|---|---|
| **Drafted by** | Abdullah Omar Saif |
| **Version** | 1.0 |
| **Date** | 28-Nov-2013 |
| **Reviewed by** | HASAN T. EMDAD |
| **Version** | 2·0 |
| **Date** | 28·11·2013 |
| **Document Type** | Public |

Mango Teleservices received accrediting of certifying authority from the office of the Controller of Certifying Authority Bangladesh dated: 19-January 2011. Mango PKI is based on a trust center under the Root Certifying authority that holds the only self signed the highest trust center of the national PKI. On today Mango Certifying Authority will perform its "Root Key Generation Ceremony" and prepare the CSR that will be signed by the Root Certifying Authority and as a consequence activate Mango's PKI to serve to the customers on issuing certificates.

As a new Public Key Infrastructure (PKI) this program requires a high level of assurance, and our designated team will apply best practices and meet certain compliance needs and ensure that the highly visible key generation ceremony progresses to completion smoothly.

The meeting minutes of this key ceremony is documented in the following sections and chapters. The meeting minutes contains the HSM bootstrapping, creating Security officer, Domain Controller and Partition users and subsequently setting up partitions and setting policies, creating trust link layer that subsequently leads to generate Mango Root Key pairs and certificate. The conclusion will be generating "Certificate Signing Request" CSR procedure.

As per licensing policy Mango Teleservices Limited will submit this CSR to the office of the controller of certifying authority to be signed by the Root CA.

The CA will become activated once the signed certificate is incorporated to Mango PKI system.

This RKGC is performed in the year 2013 due to regulatory compliance incorporating on newly assigned OID on Certificate Policy

**Venue & Date:**

28-Nov-2013, The Root Key Generation ceremony Mango Teleservices Ltd started at appx. 2 PM with pre briefing session held in the conference room. All attendees and task owners were introduced with each other before beginning the activities.

**Ceremony video Recording:**

- Video Recording by Joynto Sarkar
- All CC Camera recordings (video footage)
- Conducting computer screen recording

**Responsibility matrix of Root Key Generation Ceremony:**

| Sl. | Name and Designation | Roles/Duties |
|---|---|---|
| 1. | Hasan T. Emdad Rumi<br>Head of Technical Solution | • HSM Administrator<br>• Superadmin eToken holder<br>• Conducting overall HSM Bootstrapping and RKGC<br>• Integration to Certificate Server and CSR Generation |

| Sl. | Name and Designation | Roles/Duties |
|---|---|---|
| 2. | Kazi Al Mamun<br>Admin Accounts | • Iron Safe Custodian<br>• Iron Safe Log Registrar |
| 3. | Mohammad Selim<br>Manager | • Server Password Custodian<br>• Password and PIN keeper |
| 4. | Bannya Chanda<br>Application Engineer | • Domain Officer (DO) – Red PED Key Owner<br>• Partition Challenge Passphrase keeper<br>• Assist to HSM Administrator |
| 5. | Debabrata Sarkar<br>Senior Software Engineer | • DB1, DB2, LDAP, CRL, OCSP and Certificate Server powering up<br>• Security Officer (SO) – Blue PED Key Holder<br>• Assist to HSM Administrator |
| 6. | Tanvir Islam<br>Jr. Application Engineer | • Partition owner/user (PO) – Black PED Key Holder |
| 7. | Minarul Islam<br>AGM, Admin & Logistics | • 1st mofn key owner |
| 8. | Bushra Tasnim<br>Sr. Engineer | • 2nd mofn key owner |
| 9. | Habibul Azam<br>Manager | • 3rd mofn key owner |

**Pre installation tasks before key ceremony:**

During the session the following pre installation tasks were performed:

1. The operating system, security hardening, safenet CA software package, LDAP & ADE preparation and database has been installed and pre configured on the root CA system prior to the key generation supervised by the head of technical solution.
2. The firewall policy and security token for super administration were made readily available.
3. Attendance sheet was completed by all attendees

The key generation ceremony proceeded as follows:

**Stage 1: Initial preparation (Started at 2:08 PM):**

1. All attendees and task owners were presented in the NOC room
2. The iron safe custodian Mr. Kazi Al Mamun opened the secured iron safe and deliver the log register to Ms. Shahana Ferdous, the custodian of PED, PED keys, PED cable & serial port cables.
3. Mr. Selim the password custodian received the envelopes containing the confidential credentials.
4. The CA rack cabinet was opened. Necessary cables are connected to the HSM.
5. Mr. Hasan handed over respective PED tokens to respective users.
6. Mr. Debabrata unlocked the rack cabinet

7. Program supervisor Mr. Hasan introduces the components of the rack to the audience.
8. The PED cable was connected to the PED by Mr. Hasan. He also connected the serial cables to the conducting laptop.
9. The server password custodian Mr. Selim delivered the password envelops to Mr. Hasan.
10. Mr. Hasan checks all DB 1, DB 2, LDAP, ADE, CRL, OCSP & certificate server from a NOC terminal.

**Stage 2: Create HSM environment:**

1. The HSM administrator powers up the virtual terminal to connect the null modem serial cable with the HSM.
2. Executed PUTTY program to connect to the HSM.
3. The HSM administrator logged in with the provided password from Mr. Selim.
4. The HSM administrator verified the date and time zone and fixed the date and time zone of the HSM.
5. HSM network was observed and entered the desired IP networks to the respective interfaces.
6. DNS name server records were updated.
7. The host name record was added.
8. Verified correctness of the network setup confirmed by pinging another server, also verified certificate servers network configuration by pinging to HSM appliance.
9. NTP server was configured and enabled.
10. A new HSM server certificate was generated.
11. Bind the network trust link service.

**Stage 3: Initialize HSM (Trusted path)**

1. HSM initialization command was executed with a condition of m of n provisioning.
2. The command directed to SO Mr. Arif to insert the blue PED key to the PED.
3. A series of sequence was instructed by the PED prompt and SO PIN was created.
4. Subsequent PED prompt directs the domain officer Ms. Bushra to insert the red PED key to the PED.
5. Once the domain function is executed the PED prompts to insert first m of n Mr. Dev Sarkar and subsequently the second and third m of n functions were executed by Mr. Main & Mr. Azam.

**Stage 4: View and record HSM policies:**

1. The HSM administrator showed the HSM policies to the audience and copies it for record keeping.

**Stage 5: Create HSM partition:**

1. HSM login required and consequently SO and 2 m of n officers attended the PED.
2. The login was successful.
3. The HSM partition command was executed by the HSM administrator.

4. The PED demanded the black PED key that is partition owner Mr. Masud to follow the onscreen PED prompts.
5. The PED PIN was generated and subsequently the partition client password was displayed on the PED.
6. Ms. Bushra wrote the secret values and enveloped it and handed over this to Mr. Selim.
7. The partition creation process was completed.

**Stage 6: Record and set partition policies:**

1. The HSM administrator showed the partition policies to the audience.
2. The HSM administrator updated certain policies and showed it to the audience.

**Stage 7: Set up network trust link:**

1. The HSM appliance server certificate was imported onto certificate server.
2. The HSM server certificate was registered with the certificate server.
3. A certificate server certificate was generated and exported to the HSM appliance.
4. Registered the certificate server certificate to the HSM appliance.
5. The NTLS service was re started.

**Stage 8: Assigned certificate server to HSM partition**

1. Assigned a certificate server partition on the HSM.
2. The setup was verified from the certificate server as well as from the HSM.

**Stage 9: Root key pair and certificate generation on HSM**

1. Partition command was executed on HSM.
2. Key pair generation command was executed on the certificate server where keys will be generated on the HSM.
3. Private and public key pair was generated.
4. The generated key pair was verified from the certificate server.
5. Certificate generation command was executed from the certificate server where a certificate will be generated after answering certain questions on the command line.
6. The generated key pair and certificate were verified from the certificate server and the attributes were copied and recorded.

**Stage 10: Integration to certificate server and CSR generation: (Completed at 5:43 PM)**

1. The application server was started.
2. The application server administrative section was opened after entering the super admin e token to the conducting laptop.
3. Inside certificate servers' certificate authorities section necessary inputs, parameters, values where inserted.
4. The application CA generates certificate signing requests and a CSR file was downloaded from the system.

5. The CSR request contained "No CA chain file available".

**Stage 11: Conclusion process and completion of the ceremony:**

1. The CSR file was written into a blank CD.
2. Q/A session was conducted.
3. All PED cable, PED keys, Serial cable were handed back to Mr. Mamun.
4. Mr. Mamun, the iron safe custodian collected all the items and put them back in the iron safe.
5. Everybody signed off from log register.
6. Video recordings were turned off and respective personnel deliver the recorded files to the iron safe keeper.
7. All task owners signed on the document "Root Key Generation Ceremony of Mango Teleservices Ltd." Version 2.0, dated 28-Nov-2013.
8. Task owner Mr. Hasan signed on the document –"Mango PKI Root Key pair and Certificate Generation" version 2.0, dated 28-Nov-2013.
9. Task owner Mr. Hasan signed on the document –"Integration to certificate server and CSR Generation".
10. Announced the successfully completed the Mango CA Root Key generation Ceremony.
11. All participants left the secured NOC.

**List of attendees and witness**

| Name. | Organization and Designation | Signature |
|---|---|---|
| Hasan Tanvir Emdad Rumi | Mango Teleservices Limited<br>Head of Technical Solution | |
| Minarul Islam | AGM, HR, Admin & Logistics | 28/11/2013 |
| Kazi Al Mamun | Admin Accounts | 28/11/13 |
| Mohammad Selim | Manager | |
| Asim Bepari | Senior Engineer | 28/11/2013 |
| Bannya Chanda | Application Engineer | Bannya Chanda<br>28.11.2013 |
| Tanvir Islam | Application Engineer | Tanvir Islam<br>28.11.2013 |
| Debabrata Sarkar | Sr. Application Engineer | 28.11.2013 |
| Mashiur Rahman | AGM, ITC | |
| Habibul Azam | Manager | 28/11/13 |
| Mustafa Rahman | CCO, Platinum Communication Limited | M. Habib<br>28/11/2013 |
| Lt. Col. Muhammad Aminur Rahman | CEO, Purple Telecom Limited | 28/11 |
| A.Mannan Khan | Chairman, Mango Teleservices Limited | |
| Mir Masud Kabir | Managing Director, Mango Teleservices Limited | |
| Md. Tofazzal Hossain | Deputy Controller, Office of the CCA, Ministry of ICT, Bangladesh | 28.11.2013 |
| Mohammad Tohidur Rahman Bhuiyan | Lead Auditor, Right Time Limited | 28.11.2013 |

| Name. | Organization and Designation | Signature |
|---|---|---|
| Sabah Saera | Engineer, Mango Teleservices Limited | Sabah Saera |
| Joyonta Sarkar | Executive, Finance and Accounts, Mango Teleservices Limited | |
| Arifur Rahman | GM, Platinum Communication Limited | |