~~Confidential~~

🔐 Root Certificate Authorities Ceremony 3

[redacted], 2021

Participants

Role	Name	Signature	Date	Time

Instructions for a Root Certificate Authorities Ceremony

A Root Certificate Authorities Ceremony is a scripted meeting where individuals with specific roles generate or access the private key component of a Root Certificate Authority (or multiple Root Certificate Authorities). The script and recordings are retained and published internally to Monzo staff.

Guidelines:

1. One member of the [redacted] Squad per-ceremony will be the Ceremony Administrator who leads the ceremony
2. One person (who must be a Monzo employee) will be the Internal Witness who audits the actions of the Ceremony Administrator [redacted]
4. Admission to the Ceremony Room requires participants to be identified by [redacted] If a participant cannot be identified because [redacted] they will not be admitted to the ceremony.
5. Visitors are not permitted to attend the ceremony except with the prior approval of the Ceremony Administrator, [redacted]
6. Filming starts before the majority of participants arrive, and in any case before step 1 of this script is started.
7. Ceremony Participants follow the script step by step in order to attest to the ceremony's proper performance
8. The Ceremony Administrator reads each step aloud prior to its performance
9. Upon the successful completion of a step, the Internal Witness will announce and record its time of completion and initials the step in their script
10. Some steps during the ceremony may require the participants to recite and/or confirm identifiers composed of numbers and letters. When spelling identifiers, the NATO phonetic alphabet should be used.
11. A ceremony participant who has cause for concern or detects an issue is encouraged to interrupt the ceremony for discussion. The issue is brought to resolution before the ceremony resumes.
12. Questions and suggestions for improvement are welcome and can be discussed at any time or posted to our Slack Channel: [redacted]
13. Data is only moved between the air gapped Laptop and other Monzo systems used CD-R disks, which can only ever be written to once. All CD-R disks are retained for audit purposes.
14. **Temporary: During the coronavirus pandemic we are practising social distancing to keep everyone safe, as part of this we are:**
    a. **Ensuring there is as much physical space as possible between onsite participants**
    b. **Reducing the amount of attendees as much as possible** [redacted]
    c. **Wearing masks at all times during the ceremony where contact closer than 2 metres apart is unavoidable**

Exceptions

Unplanned events (exceptions) are evaluated, documented and acted upon. It is the Ceremony Administrator's sole responsibility to decide on proper actions after consulting with the Internal Witness.

Emergency Evacuation Procedure

- You should already be aware of the normal office health and safety and emergency evacuation policies, please ask if you aren't.

- Please follow the normal office health and safety and emergency evacuation procedures regardless of the circumstances of the ceremony. If there is a need to evacuate, leave the ceremony via the closest and safest exit to you, leaving everything behind.

[redacted]

- The Ceremony Administrator will decide on what action to take as an exception once the all clear is sounded and participants return to the ceremony.

- If an alert is heard that an evacuation may be necessary, the Ceremony Administrator may choose to interrupt the ceremony to begin securing equipment in anticipation of a possible evacuation. [redacted]

On hearing the fire alarm

- Before the fire alarm goes off, there will be an alert on the tannoy system that an alarm condition is being investigated. If you hear this alert, please prepare yourself for a potentially imminent evacuation

- If [redacted]staff do not find the source of concern within a few minutes and deactivate it, the fire alarm will sound and a building evacuation will be triggered. At this point, please leave the building via the nearest exit.

Fire Exits and Assembly point

Fire Exits:

- Fire exits are located at either ends of each Monzo floor, clearly signposted with green fire exit signage. In [redacted]

- Do not use the lifts or stop to collect personal belongings. Please use the closest and safest exit to you.

Assembly Point:

- Our assembly point is [redacted]

The NATO Phonetic Alphabet

A	Alpha	AL-FAH
B	Bravo	BRAH-VOH
C	Charlie	CHAR-LEE
D	Delta	DELL-TAH
E	Echo	ECK-OH
F	Foxtrot	FOKS-TROT
G	Golf	GOLF
H	Hotel	HOH-TEL
I	India	IN-DEE-AH
J	Juliet	JEW-LEE-ETT
K	Kilo	KEY-LOH
L	Lima	LEE-MAH
M	Mike	MIKE
N	November	NO-VEM-BER
O	Oscar	OSS-CAH
P	Papa	PAH-PAH
Q	Quebec	KEH-BECK
R	Romeo	ROW-ME-OH
S	Sierra	SEE-AIR-RAH
T	Tango	TANG-GO
U	Uniform	YOU-NEE-FORM
V	Victor	VIK-TAH
W	Whiskey	WISS-KEY
X	X-Ray	ECKS-RAY
Y	Yankee	YANG-KEY
Z	Zulu	ZOO-LOO

Required Participants

Role	Name
Ceremony Administrator	[redacted]
Internal Witness	[redacted]
Keyholder 1	[redacted]
Keyholder 2	[redacted]
Keyholder 3	[redacted]
Keyholder 4	[redacted]
Keyholder 5	[redacted]
Keyholder 6	[redacted]
Keyholder 7	[redacted]

Optional Participants

Name
[redacted]

Remote Participants (Optional)

Name
[redacted]

(The following can be verified by reviewing the recordings of [redacted], a copy of which is available in [redacted]

TEB Numbers

Name	TEB Number
[redacted]	[redacted]
[redacted]	[redacted]

Internal Tools Root

Check Certificate Signing Request (CSR) Integrity

Activity	Initials	Time
Ceremony Administrator checks the integrity of the CSR by executing **openssl req -noout -text -in ./csr/internal-tools-intermediate.csr** This will give CSR information similar to the figure below. Pay attention to the fields marked on the figure in bold (e.g. the ECDSA Key Size and Certificate Subject). Press SPACE until end of display and then “q”.		

```
Certificate Request:
  Data:
    Version: 3 (0x2)
      Subject: O=Monzo Bank Ltd, OU=Security, CN=Production Internal Tools Root CA
      Subject Public Key Info:
        Public Key Algorithm: id-ecPublicKey
        Public Key: (384 bit)
          pub:
            ...
     Attributes: a0:00
  Signature Algorithm: ecdsa-with-SHA256
    c8:11:c8:7e:12:7e:7f:da:26:0f:c1:41:a4:cd:28:84:f2:da: ... 8d:f5:9f:a2
```

Create the Internal Tools Root & Intermediate

Activity	Initials	Time
Ceremony Administrator executes the root initialization script by executing **cd /media/PKIROOT/[redacted]** **[redacted]-env=production -csr=/media/PKIROOT/[redacted]csr/internal-tools-intermediate.csr** The Ceremony Administrator will be prompted by the script to select [redacted] operator smart cards to unlock the HSM to issue the root and intermediate. **Take care to use the operator cards and not the administrative cards** Each of the [redacted] keyholders selected by the Ceremony Administrator when asked will come to the front of the room and enter the PIN for their smart card into the HSM while shielding the PIN from the camera and all other participants. Smart cards (except the last smart card inserted) will then be placed back on the key ceremony table in plain view of the camera and keyholders will return to their seats without their smart cards. **The last card inserted into the HSM should not be removed and must remain in the HSM.** List cards used below:		

Verifying the Internal Tools Root & Intermediate

Activity	Initials	Time
Ceremony Administrator verifies the issued root and intermediate CA exist by executing **ls**		
Ceremony Administrator shows the participants the issued Root CA by entering **openssl x509 -in production-internal-tools-root[redacted].pem -text -noout** Ceremony Administrator and Internal Witness verify that the Certificate is in good form, in particular by verifying the following properties: **Subject: O=Monzo Bank Ltd, OU=Security, CN=Production Internal Tools Root CA** **Public Key: (384 bit)**		
Ceremony Administrator removes the card still in the HSM and places it on the key ceremony table in plain view of the camera.		
[redacted]		
[redacted]		

Bagging Smart Cards for Keyholders

Activity	Initials	Time
Ceremony Administrator places each Smart Card into its own Tamper Evident Bag in plain view of the camera and records the Serial Number of the TEB on the table below in the script of the Internal Witness. Once sealed into the bag, Ceremony Administrator shows the sealed bag to one of the cameras, ensuring that all sides of the bag are visible to the camera and the serial number is clearly shown to the camera at least once. Ceremony Administrator places the bag containing the Smart Card on the key ceremony table		

Card No	TEB No.	Time	Internal Witness
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			

Distributing Smart Cards to Keyholders

Activity	Initials	Time
Ceremony Administrator calls each key-holder in turn up to the front of the room, Keyholder is given their Smart Card inside the TEB. Keyholder verifies the Serial Number on the TEB matches the Serial Number their smart card was placed into and signs for the smart card in the table below using the Internal Witness's copy of the script. Internal Witness initials table entry for each Keyholder.		

Card No	TEB No.	Name	Signature	Time	Internal Witness
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					

HSM1

Activity	Initials	Time
Ceremony Administrator in view of the camera inserts HSM1 into a Tamper Evident Bag and seals the bag.		
Ceremony Administrator writes on the bag [redacted] **PRODUCTION HSM1** [redacted] The Ceremony Administrator and Internal Witness sign the bag		
Ceremony Administrator says the TEB Number Record the TEB Number below: TEB Number: _____		
Ceremony Administrator holds the Tamper Evident Bag up to one of the cameras, making sure that all sides of the bag are recorded and any serial numbers are clear		
Ceremony Administrator places the Tamper Evident Bag on the equipment cart		

Return to Ceremony Room

Activity	Initials	Time
Ceremony Administrator, Internal Witness [redacted] return to the Ceremony Room with the Ceremony Administrator pushing the empty equipment cart		

Participants sign to confirm ceremony's successful execution

Activity	Initials	Time
Each participant signs in the table on the last page of the Internal Witness's copy of the ceremony script if they are satisfied that the Confidentiality, Integrity and Availability of the key material was preserved fully during the ceremony and that they have no further objections regarding the ceremony. A participant may choose not to sign if they have objections or concerns regarding the ceremony.		

Stop and preserve recordings

Activity	Initials	Time
Ceremony Administrator stops all recordings and begins saving recordings to [redacted]		

-End of Ceremony-

This is the end of the ceremony. Once you have signed the final page on the Internal Witness's copy of the script (or have chosen not to because you have objections or concerns) you are free to go. Thank you for attending the ceremony 😊

Participant Approval

Please confirm that you are satisfied that the Confidentiality, Integrity and Availability of the key material was preserved fully during the ceremony and that you have no further objections regarding the ceremony.

Role	Name	Signature	Date	Time