MRI-Secure Communication Guide – DRAFT v0.3

The purpose of this Secure Communication Guide is to assist MRI to minimize the risk and consequences of communication being intercepted ("listened to") between MRI, partner organisations and applicants.

This Secure Communication Guide outlines three steps to improve the security of communication:

1. **Basic analysis of communication risks**
2. **Tools + good practices for secure digital communication**
3. **Sequencing of secure communication tools for initial contacts with applicants**

Following this guide will NOT provide 100% security for the users nor will it cover all processes of critical communication within the MRI-program. But it will support everybody involved to take conscious decisions to improve their security for their sensitive communication.

1. BASIC ANALYSIS OF COMMUNICATION RISKS

- Check with the applicants, how they assess their own risk of their digital and phone communication being surveilled
- Check (with applicants, host organization, other sources), if it would be dangerous for the applicants, if their interactions with MRI (contact, communication, exchange of docs, money transfer,…) would get known to their adversaries
- Check with partner / host organization of their assessment of risk of surveillance in this case
- Check, if there are cases of persecution due to use of secure and encrypted apps (like Wire Messenger in Bahrain) (using local knowledge, contact FrontlineDefenders, Protectoin International etc. or use online resources like: https://www.privacyinternational.org/type-resource/state-privacy)

The objective is to balance direct secure communication with secure apps and channels versus raising suspicion by adversary.
If the applicants don't take any digital security precautions despite assessed risks, MRI takes the responsibility to introduce more secure options and steps (if these do not increasing the risk for the applicant or MRI)***.***

Assessment	**Optional steps including partner organizations**	**Digital communication steps**
For all steps including the partner organizations: Establish secure communication channels with these organizations first (checking if assessment steps 1+2 below also apply for the partner organizations!), then extend through these secure channels to the applicants if necessary.		
1 - Digital and phone communication is actively surveilled	Use in-person-meetings via host or partner organizations (establish secure communication channels with and through these organizations)	Use secure communication channels like described below. Don't use general channels like Facebook, email, phone, SMS, Skype

Assessment	Optional steps including partner organizations	Digital communication steps
2 - Secure apps are illegal or under surveillance or persecution	If possible, use in-person-meetings or channels via host or partner organizations	If 3 (Direct contact with MRI is dangerous) does not apply, you can use Whatsapp as an partially secure alternative to digitally more secure communication apps
3 - Direct contact with MRI is dangerous	Use channels via other contacts close to the applicant or through partner or host organization (establish secure communication channels with and through these channels first)	If digital direct communication is necessary, use anonymization tools like TOR and TAILS (only if these are not illegal or under surveillance!) on both sides

2. TOOLS + GOOD PRACTICES FOR SECURE DIGITAL COMMUNICATION

TOOLS

The following tools are safe to use, as long as using secure or encrypted apps and tools would not be raising suspicion or creating evidence for persecution. https://www.securemessagingapps.com provides a detailed comparison of different messengers, relating to their security.

Use case needed – generic	Tool	Info	Links to tool and instructions
Email communication secondary: file sharing	**Protonmail**	Encrypted Email – Encryption is only automatic between Protonmail-users (for communication with PGP-GPG-users this can be enabled), but can also be enabled to non-protonmail addresses – Works on phone (own apps for iOS + Android) and computer (browser based for free accounts, desktop apps for Mac OS + Windows)	https://protonmail.com/

Use case needed – generic	Tool	Info	Links to tool and instructions
Voice (or video) conversations secondary: chat, using internal pad for note taking	**Jitsi Meet**	Fully encrypted, 100% open source video / audio / chat conferencing – one-time conversations (no saving of communications after leaving the secure room) – easy to access via link, no installation necessary – needs browser (Chrome / Firefox / Safari) on computer – easier use on phones via specific iOS / Android apps – option of hosting own installation on MRI-Server	https://meet.jit.si (be aware that in the moment the most secure way of using Jitsi Meet is by hosting it on your own servers)
Messaging secondary: voice calls (2 participants), file sharing	**Signal messenger**	End-to-end encrypted messaging and call app for iOS / Android. Keeps hardly any logs. Open source. – Desktop version needs phone for registration	https://signal.org/ https://securityinabox.org/en/guide/signal/android/ https://ssd.eff.org/en/module/how-use-signal-android https://ssd.eff.org/en/module/how-use-signal-ios
Messaging secondary: chat, voice/ video calls (up to 10 participants, file sharing	**Wire messenger**	End-to-end encrypted messaging and call app for iOS / Android. Keeps some logs. Open source. – Anonymous registration possible with email-addresses – Two-three parallel accounts possible on one device – Team versions available	https://wire.com/en/

GOOD PRACTICES

Make sure your operating system (Mac OS, Windows, Linux, Android, iOS, ...) is up-to-date, and that security updates are installed automatically. (For further information about safe use of smart phones and computers, check Security in a Box or the EFF-Surveillance Self Defence Guide which you find in the resources list.
Make sure your browser (Firefox, Chrome, Safari, ...) is up-to-date, and that security updates are installed automatically.

When dealing with attachments:

- Check with sender over separate channel
- Examine the URL of the attachments (hover over link, longpress link

Don't open links or attachments without checking back over a different channel with the sender. Make sure the link destination is what you would expect (shown in the bottom left of mail applications when hovering the mouse cursor over the link, or by long pressing the link on a mobile phone).

Use plain text messages and emails (non-html) over attached documents whenever possible!

Use good passwords. Best practice is to use a password manager like KeepassXC (for Mac OS, Windows, Linux) or KeePass DX (Android) or MiniKeepass (iOS), so you can have a strong, random, and unique password for each of your accounts.

Avoid taking photographs of documents to transfer bits of information. The picture might have other information that need not be shared/saved and the photo file might have metadata that isn’t to be shared/saved

Use of messengers: Given that there could be criminalisation for using certain apps and the artist/activist might be forced to unlock their phones or computers, it is a good practice to use disappearing/time expiration of messages for transfer of extra sensitive information, like passwords and such. Also use of the messenger to just communicate and not store information. And use pin or password to lock the apps like Protonmail, Wire or Signal.

3. Sequencing secure ocmmunication tools for initial contacts with applicants

The sequencing for using secure communication channels could be these below for two scenarios:

As a result of part 1 (risk assessment, check for secure use of encrypted and secure communication channels – not to raise attention by the adversaries), these two communication sequences could be used, after the applicant contacted you by phone or email:

Scenario 1 **Establishing direct contact with applicant**	**Scenario 2** **Using partner or host organization for contact with applicant**
First online meeting with *Jitsi Meet* – link sent to applicant via *Whatsapp* or email (*Protonmail*). For hyper sensitive situations possibly password protect the Jitsi Meet channel and send the password separately from the link. → Check for additional not invited participants in the chat room and check with video chat for identity of applicant	Setup secure communication channels with the partner or host organization (including at least *Signal* / *Wire*, *Protonmail* or other encrypted email for communication and file sharing).

Scenario 1 **Establishing direct contact with applicant**	**Scenario 2** **Using partner or host organization for contact with applicant**
If continuous communication is needed, establish *Signal* or *Wire* communication or at least use *Protonmail*. If not, continue using *Jitsi meet.* Coach the applicants on how to use the respective app. If file sharing is needed, go for the apps, which support this securely. When using Wire or Signal on high sensitive information, force the use of time out / disappearing messages after informing the other party.	Applicant is invited for face-to-face meeting to the host or partner organization. Staff of that organization then communicates the content through the established secure channels to MRI.
Check with applicant during use of *Signal* / *Wire* etc., if additional support for securing their digital devices is needed. Either coach them or provide access to other resources or training (FrontlineDefenders, ...)	Alternatively, the host or partner organization provides access for the applicant using their secure communication channels with MRI
After concluding communication with applicant, make sure, that all channels are deleted from both sides.	After concluding communication with applicant, make sure, that all channels are deleted from both sides.

Additional Resources EN (online)

Digital security
https://securityinabox.org
https://ssd.eff.org/
https://www.digitaldefenders.org/digitalfirstaid/
https://gendersec.tacticaltech.org/wiki/index.php/Main_Page

Holistic security
https://holistic-security.tacticaltech.org/
http://integratedsecuritymanual.org/
https://capacitar.org/capacitar-emergency-kit/

Additional Resources ES (online)

Digital security
https://securityinabox.org/es/
https://ssd.eff.org/es
https://gendersec.tacticaltech.org/wiki/index.php/Main_Page

Holistic security
https://www.alunapsicosocial.org/single-post/2017/04/06/Modelo-de-Acompa%C3%B1amiento-Psicosocial-ALUNA
https://capacitar.org/capacitar-emergency-kit/

Additional Resources FR (online)

Digital security
https://securityinabox.org/fr/
https://ssd.eff.org/fr

Holistic security
https://capacitar.org/capacitar-emergency-kit/