

Encrypted communication on the MPo2

Instruction manual

Contents

Part one

- 4** Encrypted calls on the MPO2
- 6** Installing the software and registering with Signal
 - 6 Preparation
 - 6 Installing the Pigeon encryption software
 - 6 Activating Pigeon and registering with Signal
 - 8 Setting a passcode (PIN)
 - 8 Securing the Signal account
- 9** Settings
 - 9 Profile
 - 9 Notifications
 - 9 Privacy
 - 10 Attachments
 - 10 Storage
 - 10 Advanced
- 11** Contacts
 - 11 Review auto-added Contacts
 - 11 Inviting people to start using Signal
 - 11 Confirm connections with other Signal users ('exchange private keys')
 - 12 Refresh
- 13** Spoken communication
 - 13 Making calls
 - 13 Voice messages
 - 14 Search
 - 14 Reset secure session
- 15** Written communication
 - 15 Text messages
 - 15 Conversations
 - 16 Mark all read
 - 16 Archiving or deleting conversations
 - 16 Groups
- 19** Other features
 - 19 Attachments
 - 19 Note to Self
- 20** Advanced settings
- 21** Appendix 1: list of symbols
- 22** Appendix 2: Lost passcode

About this instruction manual

— Version

1.0 (based on Pigeon
version 1.0776)

— Revision date

March 2021

— Change

First version

Encrypted calls on the MPO2

Signal: bringing true encryption to the world of communication

The Signal Foundation

Signal is a telecommunications platform with roots that go back to 2010. It is run by a registered non-profit organisation, the Signal Technology Foundation (usually shortened to ‘the Signal Foundation’). They are based in California, USA.

The Signal Protocol

The Signal Protocol is an encryption system developed and used by Signal. It is also licensed out to other companies, such as WhatsApp/Facebook and Skype. However, there are differences in how it is deployed. Signal stands out in two ways. Firstly, the ‘metadata’ (who called whom, when, on what type of device, etc.) is also 100% encrypted/unavailable – instead of being harvested and sold. Secondly, encryption is always activated: it is never necessary to select it as an extra option.

The Signal application

This is a free app that can be installed on almost all desktop/laptop computers, tablets and smartphones. It gives access to the Signal network.

The Signal network

The Foundation’s servers and the millions of people with Signal-compatible devices together constitute a global network that anyone can join free of charge. Unless specified otherwise, all references to Signal in this document refer to the Signal network.

Pigeon: bringing Signal to the MPO2

Pigeon is closely based on the Signal app. It is designed specifically for accessing the Signal network from a voicephone: small screen and a keypad-only interface. Inevitably, some elements of Signal are not provided; the focus is on high-quality encrypted phone calls, with encrypted messaging also available.

Pigeon provides encrypted communication with any other Signal user, to the same level of security. Signal calls are Internet-based (VoIP), which means that they are free of charge (apart from any data charges that may arise).

This instruction manual: bringing Pigeon to the owners of MPO2s

The MPO2 does not have a Help feature. The text-based interface is very quick to use, once it is mastered, but in general it is not guessable. This manual needs to be worked through carefully, from the beginning until the end. In addition, it assumes full knowledge of the MPO2's main instruction manual. More information about Signal, any known software bugs, pending new features, etc., are available on the Punkt. website's Support section.

The MPO2: bringing the focus-friendly option to the Signal network

Using Signal on the MPO2 means foregoing a number of secondary features. But sometimes it is good to take a break from smartphones. And now it is possible to do that without missing out on the world's leading communication encryption system.

Installing the software and registering with Signal

Carefully read this section to the end before commencing the set-up process.

Preparation

There are two separate stages to setting up encrypted communication on the MPO2: installing extra software, called Pigeon, and then registering with Signal. Before proceeding, the following are required:

- **Up-to-date operating system** on the MPO2 – v2.0 (v02.00.0082) or later.
- **Connection to the Internet** (preferably with both methods available: Wi-Fi for downloading the software and then via the MPO2's own 4G LTE connection for registering with Signal).
- A **phone number** that can be used to receive a one-off unencrypted SMS text message or unencrypted automated voice message. This does not need to be the MPO2's phone number, although the registration process is slightly simpler if it is. However, for as long as it is linked to a Signal account it will not be available for anyone else to use with Signal. Also, it will be visible to any other Signal user with whom messages are exchanged (a prerequisite for making phone calls).

Installing the Pigeon encryption software

1. Connect the MPO2 to a power source, or ensure that its battery is at least 30% charged.
2. Connect to the Internet via Wi-Fi or the MPO2's 4G LTE data connection, as preferred. (Wi-Fi may avoid unnecessary data charges.)
3. From the Main menu, select Settings, then Applications, then Manage.
4. Wait for a few seconds while the MPO2 checks for available software.
5. When 'Pigeon' appears on the screen (scroll to find it, if necessary), select it.
6. Wait while the software is downloaded and installed.
7. When a message appears stating that the installation process has finished, press the Punkt. key to return to the Home screen.

Activating Pigeon and registering with Signal

1. If the Internet connection for the software installation was via Wi-Fi, reconnect using the MPO2's 4G LTE connection if possible. If doing so while abroad, be sure to activate data roaming. (Wi-Fi can be used if necessary, but the authentication process may be more complicated.)
2. From the Main menu, select 'Pigeon'. (Short-cut:

long-press the Message key from the Home screen.)

3. Read the Software Disclaimer and Terms of Use and Privacy texts, and then select 'Continue'.
4. Select 'Allow' to permit Pigeon to access the MPO2's Contacts list, use and record audio, view SMS, access photos/media/files and make/manage phone calls. More information about this is available in the Support section of the Punkt. website.
5. The next step is to enter a phone number (mobile or land-line) suitable for receiving a one-off, unencrypted verification code from Signal (SMS text or auto-generated voice message). The Signal account will be linked to this phone number. It does not have to be the number of the MPO2 that is currently being set up; it can only be linked to a single Signal account. If the correct country code has been automatically displayed, scroll down and select 'Next'; otherwise press the Punkt. key and use the search feature to find the correct code. Enter the phone number itself, omitting the initial zero, and select 'Next' to send the account request to Signal. (From this point on, do not press the End key until a Signal Profile has been set up as this will cancel the registration process and a new account request will need to be sent.)

6. When the request is received by Signal, there may be a requirement to negotiate a 'Captcha' test in order to demonstrate that it is a bona fide registration attempt. The test requires the registrant to select from a range of images, according to a specific instruction. Use the 2, 4, 6 and 8 numerical keys to a) locate all the images that have been sent (not all will be visible on the screen at once) and b) highlight an individual image so that it can be selected by pressing the Punkt. key (or the 5 key). If the images fail to load, press the 0 key to refresh. (This can also be done if a 4x4 image test is loading; there is a possibility that the replacement will be the easier 3x3 format.) When all the required images have been selected, press the 6 and 8 keys to move down to highlight what may either be 'Verify' or 'Continue' (depending on which version of the Captcha test has been sent) and press the Punkt. key.
7. Once the Captcha test has been passed (it may take a few attempts), Signal will then send an unencrypted SMS message containing the verification code to the number that has been provided (there may be a short delay). Confirmation that this has been received needs to be sent back to Signal:
 - a. If the phone number that was entered is that of the MPO2 currently being set up, the

MPO2 will autofill the confirmation receipt text box automatically (dismiss the SMS notification). Select Next to send confirmation of receipt to Signal.

- b. If a different phone number has been used, the verification code needs to be returned manually. If the number is for a phone that can receive SMS messages, simply copy the code into the MPO2 over the greyed-out text and select 'Next' to send confirmation of receipt to Signal. If the phone cannot receive SMS messages (i.e. is a land-line phone), scroll down and select 'Call me instead' to request an auto-generated voice message that reads out the verification code (this option disappears when there are six digits in the text box, there is a 60-second countdown before it can be used, and a second Captcha test may be required). When the call comes, note down the code and send it back to Signal as described above.
- c. If the confirmation code does not arrive, check the phone number that was sent to Signal by scrolling down and selecting 'Wrong number'. The phone number will be displayed, and it can be edited and resent if required. If it shows the correct number, check with Signal (their website and social

media) to see if there is a problem with their server.

- d. If an incorrect code is sent to Signal, the text entry box will reappear.
8. Re-registering only: if the phone number is already linked to a Signal account that requires a PIN, this will be requested at this point.
9. Create a Signal Profile by filling in the 'First name' (mandatory, can be a nickname) and 'Last name' (optional) fields. These will be sent (encrypted) to recipients of all calls and texts, but are not sent to the Signal Foundation. Use the Up and Down keys to move between the text fields. (It is not possible to have a Signal Profile image when using the MPO2.) Scroll to and select 'Save' to finish the registration process.

Further information about registration is available on Support section of the Punkt. website.

Setting a passcode (PIN)

IMPORTANT It is essential to set a Signal passcode before commencing use of the Signal service. It is necessary for two reasons:

1. To enable subsequent locking of the Signal account, i.e. protecting it from being taken over by a third party.
2. To assist with setting up Pigeon again, in the event of it being deleted and then reinstalled.

To set the passcode:

1. From the Pigeon menu, select 'Settings', then 'Privacy', then 'Create a PIN'.
2. Decide on passcode, and make multiple secure copies of it. It can be numerals-only or a combination of numerals, letters and special characters. It should be unrelated to real-world things like birthdates, and not used for any other account. A password manager with two-factor authentication is recommended.
 - a. For a numerals-only passcode, simply enter a PIN of at least four different digits (no single-step ascending or descending numbers, e.g. 3456 or 8765).
 - b. Alternatively, scroll down (press the Down

key once, then the Punkt. key – the text does not highlight prior to selection) and select 'Create alphanumeric PIN', then scroll back up to recreate the cursor above the line and enter a passcode comprising at least four letters, numbers or special characters (the last can be accessed by pressing the Star key).

- c. Whichever format is chosen, the characters should be observed very carefully while they are being entered (they are only visible for a short time), lest an input error occur twice in a row. Work slowly, and be particularly alert to a character being accidentally duplicated or omitted.

3. Scroll down and select 'Next' and re-enter the passcode, again checking the characters as they are entered. The MPO2 will then encrypt the passcode and send it to the Signal server.
4. Reminders: the MPO2 will occasionally and with decreasing frequency prompt the user to re-enter the passcode as a way of assisting with the memorisation process. It is recommended that this feature be left on.

Securing the Signal account

Finally, it is essential to protect the Signal account from being taken over by someone else, by 'locking' the

registered phone number to the account. This process requires that a passcode has been set, as described above.

- Staying in the 'Privacy' sub-menu, select 'Registration Lock'.
- Scroll down and select 'Turn on'.
- Check that 'Registration Lock ON' is showing in the 'Privacy' sub-menu.

Note: a Signal account is only as secure as the phone that it is linked to. For maximum security, ensure that the MPO2's auto-lock feature and passcode protection are activated at all times.

Settings

From the Pigeon menu, select ‘Settings’ and go through each sub-menu in turn.

Profile

This displays the Signal Profile (user name), which is what will be shown when communicating with other Signal users. Review it, and then use the Back key to exit. (If a text box is highlighted, it will be necessary to press the Back key repeatedly. The content of the text box will appear to be deleted but no changes will be saved.) To amend the Signal Profile, scroll between the text boxes and then select Save to finish.

Notifications

Different sounds can be specified, and vibrating alert activated/deactivated, for:

- a. messages
- b. calls
- c. ‘Signal events’. (On the MPO2, ‘Signal events’ refers solely to when someone in the MPO2’s main Contacts list joins Signal)

It is strongly recommended that the ringtone and the message notification sound for incoming Signal calls and texts be changed, in order to demarcate them from unencrypted calls and texts. The MPO2’s full range of notification sounds is available to choose from; a filled white circle indicates which sound is set.

Privacy

Communication

- **Always relay calls** When using Signal, calls are always encrypted. Callers do not see each other’s IP addresses, but if the necessary steps are taken these can be obtained by them, and potentially also by a third party with access to sophisticated techniques. When ‘Always relay calls’ is selected, calls will be relayed via Signal’s servers (similar to a VPN). This makes it impossible to obtain the other party’s IP address. However, relaying calls may cause some increase in latency and reduction in audio quality. Press the Punkt. key to turn this feature on if maximum security is desired; its on/off state will be displayed within the horizontal-scrolling text. Select it again to turn off.
- **Read receipts** A pair of filled ticked circles above a sent message indicates that it has been opened on the recipient’s device (and has most likely been read, hence the feature’s name). ‘Read receipts’ could also be described as ‘Opened indicators’. For the feature to function, both parties need to have it turned on. Deactivating it on the MPO2 will remove all read receipts from the device itself, but will have no effect on any read receipts that may be found on other devices showing which messages have been received by and opened on the MPO2 in the past. On the other

hand, activating the read receipts feature is retrospective: if messages have been exchanged with it turned off and it is then turned on (on both devices), read receipts will appear above all messages received from the other party, on both sides, in all conversations. (This change is only triggered when both devices are connected to the network simultaneously.)

- **Typing indicators** When active, an animated ellipsis next to a Contact’s Signal Profile image indicates that they are composing a message. Again, this will apply to both sender and recipient and will only appear when both parties have it switched on. Its state is indicated within the sub-menu. Simply select it to deactivate or reactivate it according to preference.
- **Generate link previews** A link preview is an image taken from the website that has been linked to. It is created when a message is being composed and a link to one of a list of popular websites has been included; an associated thumbnail image is automatically obtained from the linked-to website (assuming the general Attachments settings permit this for the current type of Internet connection). Data usage is minimal. Turning it off will not prevent the receipt of link previews from other devices; this can be achieved within the Attachments sub-menu, described below.

- **Blocked Contacts** Selecting this will display the linked phone numbers of any Signal Contacts who have been blocked. To block a Contact, select ‘Add blocked user’, select their name from the list and then select ‘Block’. To unblock a Contact, select their Signal-linked phone number (doing this will reveal their Signal Profile) and then select ‘Unblock’.

Sealed sender

This refers to whether the sender’s address is hidden. This has for some years been inherent within the Signal system.

- **Display indicators** If activated, an indicator will be displayed above a message to show that it was sent with Sealed Sender activated. Because this feature is now pretty much universal, this option can in most cases be left switched off.
- **Allow from anyone** If this is turned off, incoming messages from senders whose Signal-linked number is not in the MPO2’s main Contacts list will be automatically blocked and deleted. The sender will be informed that the message has not arrived. In order to start communication, their Signal-linked phone number must be added to the MPO2’s main Contacts list. After a short period (or immediately, if ‘Refresh’ is selected from the ‘New message’ sub-menu), their Signal Profile name will become visible within the Pigeon Contacts list and messages can be received.

Pigeon PIN

It is essential to have a) created a numeric or alphanumeric Signal passcode (PIN), and b) activated Registration Lock in order to protect the Signal account being taken over by a third party. If this has not already been implemented, follow the instructions described above.

- **Change your PIN** Selecting this will cause a repeat of the initial setting-up process. It can be exited by pressing the Back key.
- **PIN reminders** These are generated by Pigeon to help ensure that the passcode (PIN) is memorised effectively. If preferred, they can be deactivated.
- **Registration Lock** This should be kept on at all times, but if it is necessary to turn it off, this can be done here.

Attachments

This governs whether the MPO2 automatically accepts files enclosed with messages (images, audio, video or documents – always automatically encrypted), when its Internet connection is via each of the three options of mobile data (home country), mobile data (roaming), and Wi-Fi. If the current Internet connection changes, the MPO2 will automatically accept any pending attachments that are compatible with the settings for

the new connection. The acceptance settings can be overridden: an attachment can be accepted at any time by selecting it within its accompanying message. Attachments (and messages) are sent via the Signal server, and will be held there for at least seven days.

Documents cannot be opened on the MPO2, but it is possible to forward them to another device for viewing there.

Storage

This refers to how long received messages are retained by the MPO2. Settings apply to all messages and are entirely optional.

- **Keep messages** Sets a time limit for how long messages are retained.
- **Conversation length limit** Defines the maximum number of messages that are retained. Once the limit is reached, oldest messages are automatically deleted. A single limit applies to all message threads.
- **Clear message history** Permanently deletes all received messages and media.

Advanced

Information about Advanced settings is provided at the end of this document.

Contacts

Review auto-added Contacts

As soon as Pigeon is installed, it creates a Signal Contacts list by automatically identifying which phone numbers in the MPO2's main Contacts list are linked to Signal accounts. Signal Contacts can only be included in the Signal Contacts list if they are already in the MPO2's main Address Book. This means that Signal communication can only begin once the recipient's Signal-linked number is in the MPO2's main Address Book.

Signal Contacts are all shown, in alphabetical order, below the 'New message' menu (and also in the 'New group' menu). Note that if someone has given themselves a different name for their Signal Profile it will be converted to the name they have in their entry in the MPO2's main Contacts list. Also, individuals who are in the MPO2's main Contacts list will not appear in the Signal Contacts list if their Signal account is linked to a phone number that is not included in the main list.

Inviting people to start using Signal

A pre-written text message is available, inviting people to start connecting via Signal. It is ready to be sent (in standard, unencrypted SMS format) to anyone who is included in the MPO2's main Contacts list but whose

listed phone number is not already linked to a Signal account; it can be sent to people individually or collectively.

- If sending to multiple Contacts, make a separate note of their names.
- From the main menu, select 'New message' and then 'Invite Contacts'.
- Read the horizontal-scrolling message. (It is not possible to edit it.)
- Select 'Share with Contacts'.
- Select the Contact(s) to whom the message is to be sent. Contacts whose phone numbers are already linked to a Signal account will not be listed. As each Contact is selected, the circle next to the name will change from unfilled to filled.
- Select 'Send SMS to', and then 'Yes' to confirm.

Confirm connections with other Signal users ('exchange private keys')

In order to be able to make a Signal phone call to a Signal Contact, it is necessary to first exchange text messages (a minimum of one each way). This is done in order to 'exchange private keys', which ensures that people are talking to whom they think they are and is a

necessary step for enabling Signal's exceptionally high level of security. The messages do not have to be retained afterwards, but in situations where the Contact's Signal-linked phone number is not in the MPO2's main Contacts list (and therefore in the Signal Contacts list), this message thread will be the only way of communicating with the Contact and the only record of their number.

It is strongly recommended that the process of exchanging private keys with all Signal Contacts be carried out as part of the Pigeon installation process, creating a separate list of Contacts and working through it methodically until completion. This should be done in conjunction with establishing which MPO2 Contacts have a different phone number registered to Signal and are therefore not appearing in the list of Signal Contacts, which Contacts are not registered to Signal at all and should perhaps be encouraged to join, informing people that Signal is being used via a voicephone and some smartphone-based features are not available, etc. If a Contact's Signal-linked number is different from their main telephone number(s), and is not used for any other purpose, the MPO2's custom label feature can be used to list it as 'Signal'. Note also that Contacts who are already Signal users will have automatically been alerted to the fact that this MPO2 is now contactable via Signal.

If required, it is possible to ascertain whether private keys have been exchanged with a Signal Contact by seeing whether a safety number has been created and shared with them. This is done via ‘Conversation settings’ in the Conversation contextual menu.

Exchanging private keys with a Signal Contact :

- From the main menu, select ‘New message’, scroll down and select the recipient’s name as listed with Signal.
- Enter a message, and press the Punkt. key. (It may be useful to include a reminder that a reply is necessary before it is possible to make calls.)
- Scroll down and select Send.
- Await a reply. When it arrives, the process is complete and it is possible to start making Signal calls.
- If the other person happens to send the initial message first, from the main menu simply scroll down to their name. Select it, compose a message, and select Send.

Refresh

Changes to the list of Signal Contacts may take a short while to appear. If a Contact, whose phone number is

linked to Signal, has only recently been added to the MPO2’s main Contacts list, it may be worth selecting ‘Refresh’ will cause the MPO2 to update the Signal Contacts immediately. This will also establish whether any Contacts have very recently deregistered from Signal.

Spoken communication

The Signal protocol has its roots in a messaging-only service; the ability to make calls was added later. For that reason calls are most easily made via the list of Conversations.

Making calls

A pre-written text message is available, inviting people to start connecting via Signal. It is ready to be sent (in standard, unencrypted SMS format) to anyone who is included in the MPO2's main Contacts list but whose listed phone number is not already linked to a Signal account; it can be sent to people individually or collectively.

- There are three ways of making a call:
 - a. If a Contact is listed in the Active Conversations List (or the Archived Conversations List) below the main menu, highlight their name and press the Call key.
 - b. Any Contact can be called by selecting 'New message', scroll down and select the Contact, and – with the message composition box visible but with no text in it – press the Call key.
 - c. A third option is to select 'Call' within the contextual menu available when a Conversation is displayed. This can be useful

when text has been entered into the message composition box but a reason exists for not sending it.

- To end the call, press the End key.
- Various options are available by scrolling down to the contextual menu that appears during phone calls:
 - a. Call volume level (select, adjust by pressing the Up and/or Down keys, and then press the Back key)
 - b. Hands-free speaker
 - c. Mute (turns off the MPO2's microphone)
 - d. End the call (useful in situations where the End key has become soiled)

Voice messages

To send a voice message:

- Select a Contact or Group from the Active Conversations List below the main menu.
- Scroll down to the contextual menu and select 'Voice message'. The MPO2 will immediately begin recording, while displaying a timer showing the duration of the message.
- When the message has been recorded, press the

Punkt. key. This will immediately encrypt the recording and send it to the recipient(s).

Alternatively, cancel by pressing the Back key.

Received voice messages operate exactly like standard audio files received as attachments to written messages (see below), and follow the same settings specifying whether they are automatically accepted via different types of Internet connection.

To listen to a voice message:

- Select the notification that appears on the MPO2 Home screen (depending on settings), stating that there are new Pigeon messages.
- This will lead to the Active Conversations List, highlighting the Conversation with the most recent activity.
- Select this or any Conversation. This will open it and highlight its oldest unread message.
- When a voice message is located, select it to have the message begin to play. Press the Punkt. key again to pause it.
- To cause the play position to jump back to the beginning, leave that Conversation, re-enter it, and scroll back to the voice message.
- To adjust the volume level at which voice messages are played, adjust the general phone volume via the Home screen then Settings menu.

Search

- The MPO2's Pigeon search feature presents its results in the following sources, in this order:
 - a. Names of Contacts with whom there are current conversations.
 - b. Names from the Contacts list overall (some duplication with the results from conversations).
 - c. Words extracted from the content of individual messages.

Reset secure session

This refreshes the connection with the other Signal user, which is sometimes required by the Signal network.

Written communication

Text messages

Signal text messages are always encrypted. They are always sent via the Signal server, so there is no relaying option as there is with calls.

Sending a text message:

- Select a Contact (or a Group – see below) from any of the following.
 - a. an existing Conversation (message thread) in the Current Conversations List (CCL) below the Main menu, if applicable (usually the quickest option)
 - b. the full list of Contacts accessible by selecting ‘New message’ from the main menu and searching or scrolling down (if there is already a Conversation with that Contact, this will automatically jump to the end of it)
 - c. the list of archived message threads, if applicable
- Write the required message in the message composition box that will appear.
- Press the Punkt. key or the Call key to immediately send the encrypted message. (Pressing the Call key with no text entered will cause the MPO2 to make a Signal phone call instead.)

- The text composition box can be exited without deleting entered text by repeatedly pressing the Up key until the beginning of the text is reached, and then pressing the Back key. In predictive text mode, it will be necessary to finish entering a word before the Back key can be used in this way.

Conversations

Sending an initial message will cause a conversation to be created. Beneath the main menu, the MPO2 displays a list of the individual Contacts and Groups with whom a Conversation is ‘active’, i.e. not archived. Conversation partners are listed in chronological order; Conversations with the most recent activity are shown first. There can only ever be one Conversation per individual Contact or Group at any one time.

A conversation can be archived by long-selecting and then selecting “Archive selected”. To de-archive a conversation, send a message within it. Receiving a message within it will have the same effect.

A conversation can be deleted by long-selecting it and then selecting “Delete selected”. Contacts will not be deleted by doing this, and it will still be possible to make phone calls (no need to exchange messages again).

Selecting a Conversation from the list will bring up the

message composition box, with the previous sent and received messages above it. A message can be sent by pressing the Call key or by selecting Send from the contextual menu below where it is also possible to create a voice message or make a call.

Various Conversation options are available via the contextual menu. Their settings are specific to the currently-displayed Conversation, and if it is deleted they will return to their default states. Note that when in predictive text mode, an unfinished word will prevent the Down key from being available for scrolling down to the contextual menu.

Conversation settings

- **Disappearing messages** Causes messages to self-delete from the recipient’s device after a preset time (beginning from the moment that the message is opened). It is not retroactive: messages sent prior to activation will remain.
- **Mute notifications** Silences the alert sound and prevents notifications relating to that thread from appearing on the MPO2’s Home screen.
- **Custom notifications** Applies different sounds and vibrating alert state specific to that Conversation.

- **View safety number** This is a security feature that enables users to check that they are communicating with the person they think they are. Selecting this and scrolling down will reveal a long number that should match the other person's safety number. If their device can read QR codes, they can use it to scan the code displayed above the safety number.
- **Block** An alternative way of adding a Contact or Group to the 'blocked' list, in addition to via the Privacy sub-menu described above.

Disappearing messages As above.

Reset secure session This refreshes the connection with the other Signal user, if required due to difficulties with the Signal network.

Add to Contacts This adds the Signal Contact to the MPO2's main Contacts list, by either creating a new entry or adding to an existing one as preferred. Only the phone number is transferred, and it should be borne in mind that this number may not be the Contact's number for use other than for Signal identification purposes. If this is the case, it can be marked as such by using the MPO2's custom label feature.

Mark all read

- In the CCL, the number of unread messages in each

Conversation is represented by a becircled number. If all messages in the Conversation have been opened, a temporal statement indicates how many hours ago or on what date the most recent message was sent from or received by the MPO2.

- Selecting 'Mark all read' will remove the unread message counts. If 'Read receipts' are enabled, these will be triggered – including on senders' devices as applicable.

Archiving or deleting conversations

Conversations can be archived or deleted in order to keep the list of current conversations short and easier to look through. Contacts will not be affected, and phone calls with recipients will still be possible.

- To archive or delete a Conversation, long-select it and select the desired option.
- The list of archived Conversations can be viewed by selecting 'Archived conversations' below the list of current conversations on the Pigeon main menu.
- A Conversation can be dearchived either by a) selecting it and sending a message or b) long-selecting it again.
- There is no way of retrieving a Conversation once it has been deleted.

Groups

Signal Groups are stored on the Signal-registered devices of each member. Any member can send a recorded or written message; this will be received by everyone who is in the Group. It is not possible to have Group phone calls.

Creating a Signal Group

1. To create a Group, select 'New group' from the main menu.
2. Either by scrolling or using the search feature, select the Contacts who are to be added to the Group. (The list of Contacts is a duplicate of the one available by selecting 'New message'.) As each Contact is added, the circle next to their Profile name will change from unfilled to filled. Select again to undo.
3. When all the required Contacts have been added, select 'Done'.
 - Enter a name for the Group.
 - The MPO2 will be in predictive text mode; change to multi-tap or numerical by pressing the Hash key (long-press to change language). Unusual characters can be accessed by pressing the Star key.
 - If possible, choose a name short enough to fit onto the MPO2's screen.

- Be aware that because there is no central register of Signal Groups, it is possible for Groups to have the same name as each other and some people be members of both. For this reason, a distinctive name may be beneficial. (If there is a problem with members being in namesake Groups, the name can easily be renamed in the future.)
4. When finished, select ‘Create group’. The MPO2 will display a message input box, ready for sending a message to the Group. If desired, exit by pressing the Back key.
 5. Check how the Group name looks in the CCL, including when it is highlighted, and consider adjusting its length (see below for information on how to do this).

New members

- In order for a Signal user to join the Group, they need to be added either by any member or specifically by members with administrator privileges, depending on the Group’s settings. If necessary, their Signal-linked phone number can be provided to an administrator or the administrator’s phone number can be provided to them.
- If the includee has never exchanged messages with

the includer, they will not be added immediately; they will instead receive an automated message requesting confirmation.

Using a Signal Group

- Messages can only be sent to the Group by replying to a Conversation – either in the CCL or the Conversation archive. Groups are not included in the Contacts list below ‘New message’.
- A Group Conversation can be archived or deleted in the same way as one-to-one Conversations. If a Conversation is deleted, messages to the Group will still be received and the first one that arrives will create a new Conversation. It will not be possible to post to the Group from the MPO2 until this new Conversation has been created; if desired, this can be requested of another member.
- Members can be appointed as administrators by selecting ‘Edit group’, selecting their name, and then selecting ‘Make admin’.
- A Group can be dissolved by ejecting all members apart from one administrator. This final member cannot leave the Group, because they would have to appoint another administrator. Deleting the Group’s Conversation at this point means that it can never be seen on the MPO2 again, or ever posted to from any

device. The Group’s Conversation will remain on ex-members’ devices unless they also delete their copies.

When a Group Conversation is displayed, the Conversation contextual menu contains the following extra items.

Conversation settings

- ‘Mentions’ – choose whether to receive notifications when mentioned (together with an ‘at’ symbol) in a message posted to the Group
- ‘Add members’ (only effective if the user has administrator privileges) – specify whether ordinary members (not administrators) can add new people to the Group.
- ‘Edit Group info’ (only effective if the user has administrator privileges) – specify whether ordinary members (not administrators) can amend the Group’s name, replace the profile image (on certain devices), create a Group link (on certain devices) and eject other members.

Edit group

- Change the Group’s name.
- Add new members to the Group.

Leave group

- . Selecting this means that it is no longer possible to send messages to this Group, and new messages sent to it will no longer arrive.
- . It will not delete the Group's message thread on the MPO2; this can be done separately.
- . Readmission to the Group will need to be effected by another member.
- . If departing from the Group would leave it without an administrator, a replacement will need to be appointed first.

There is no way of creating back-ups of Signal Contacts, settings or received messages. The MPO2's main Contacts list should be backed up regularly, so that in the event of loss of the phone, these can be reinstalled.

Other features

Attachments

Message attachments up to 100 MB in size can be received by the MPO2, but not created and sent (received attachments can be forwarded). Only images, videos and audio files can be opened; as described in the Settings section, documents cannot be opened but it is possible to forward them on to another device. In the current version of Pigeon it is not possible to delete an attachment or delete the specific message it is attached to; it is only possible to delete the entire Conversation.

Attachments that have not yet been accepted are represented by a downward-facing arrow, with the exception of audio files: these are shown as an empty time-amplitude graph ready for a waveform to be added to it. Depending on the settings, an attachment may not be auto-accepted; it can be manually downloaded at any time by selecting it within the message to which it is attached.

Attachments are displayed within the message box of the message they were sent with. Images will generally not fit within the screen and need to be scrolled through. They can be viewed in their entirety, shrunk to fit the screen, by being selected – press the Punkt. key a second time to remove the text shown at the top of the screen. Press the Back key to return to the Conversation.

Audio files cannot be played via the hands-free speaker. The volume level can be adjusted via the MPO2's main 'Phone volume' control, accessed via the 'Settings' menu from the Home screen. 'Play' and 'pause' are selected by pressing the Punkt. key. To return to the beginning, exit and re-enter the thread: this will cause the audio attachment to reset. If it has some text with it, this can be noted and then located by using the search feature, as an alternative to scrolling back to it.

The minimalist video playback feature is controlled by pressing the Punkt. key to play and pause. There is no fast-forward or rewind feature; the video will reset to the beginning once it has played to completion.

Note to Self

This also leads to the message composer screen, with exactly the same options below (including voice messages) and is designed for creating aide-mémoires. A series of notes can be created, written or audio. They are shown in the form of a standard thread of messages, and are accessed in the same way: via the Current Discussions List below the main menu.

Advanced settings

- . **Pigeon messages and calls** This displays the phone number to which the Signal account is linked, and allows Pigeon to be deactivated/reactivated (but not deleted – that can be done by the MPO2’s ‘Applications’ menu). If Pigeon is deactivated, other users will not be able to contact the MPO2 via Signal; any message threads that exist on their devices will be unaffected. Assuming a PIN is set and the Signal account is locked, the phone number and its associated account will be protected against third parties taking it over, but to begin using Signal communication again it will be necessary to go through the registration process and Signal Profile creation once more.
- . **Advanced PIN settings** Enables/disables PIN protection. In almost all circumstances, the PIN should be left enabled. It is required for a) locking the Signal account against someone else taking it over, and b) reinstating settings, Contacts lists and Group memberships (not messages) in the event of Pigeon being deleted and reinstalled.
- . **Pigeon [version number] upon Signal [version number]** Shows which version of Pigeon is installed and which version of Signal it is based on.
- . **Delete account** This causes the MPO2’s linked Signal account to be completely deleted, with all data

removed: linked phone number, date of first registration, date of most recent use. Unless the account has previously been locked, the associated phone number will immediately become available for anyone to use with a new Signal account. Assuming the number has not been claimed, the account can also be reinstated immediately.

Appendix 1: list of symbols

-  **Unlocked padlock**
Shows that a message has not been encrypted
-  **Animated ellipsis**
Someone is composing a message (this can be deactivated)
-  **Dotted, unfilled circle**
Message is being sent
-  **Single unfilled, ticked circle**
Message has been placed in the outbox folder, ready for transmission
-  **Pair of unfilled, ticked circles**
Message has been delivered
-  **Pair of filled, ticked circles**
Message has been opened by recipient (only shown if both sender and recipient have read receipts enabled)

-  **Unfilled circle with moving 'timer countdown' indicator**
Message is in the process of self-destructing
-  **Cancelled loudspeaker**
The thread has been muted (no notifications)
-  **Envelope symbol partially obscured by a rectangle**
Message sent using Sealed Sender
-  **Downward-pointing arrow**
A message attachment that has not yet been accepted
-  **Head and upper torso with '+' symbol**
Someone in the MPO2's main Contacts list has joined Signal

Appendix 2: Lost passcode

The passcode is necessary for two things: recovering settings, Contacts lists and Group memberships in the case of Pigeon being deleted and reinstalled, and re-registering a number when that number is subject to a registration lock.

If the passcode is entered incorrectly ten times in a row, Pigeon will be locked and further attempts will only be possible once every 24 hours.

As a necessary consequence of the exceptional level of security that Signal provides, there is absolutely nothing that either the Signal Foundation or Punkt. can do to help if the passcode is forgotten and no record is available. There is no way of a) recovering the passcode or b) circumventing the need to enter it in order to access encrypted messages, attachments and settings.

If the passcode is irretrievable, the following steps will create a fresh install of Pigeon. All content will be permanently lost, but the new Signal registration will be linked to the same phone number as before. The nearest there is to message recovery is to ask Contacts to help by resending messages and attachments they have previously sent or received. This should be requested as soon as possible, lest they be automatically or manually deleted from those Contacts' devices.

1. From the MPO2's main menu, select 'Settings' >

'Applications' > 'Manage' > 'Pigeon', and then select Uninstall. (If the passcode were available, this would result in only the loss of Contact verifications; everything else would be recovered by reinstalling Pigeon and entering the passcode.) The act of uninstalling will send a message to the Signal server, telling it to cancel the registration of the linked phone number after seven days unless there is an attempt to re-register to that number before those seven days have passed. (If an attempt is indeed made, this will cancel that request to the server.) All records (registered phone number, date of registration, date of most recent use) will also be deleted at that time.

2. At some point during the subsequent week, download Pigeon again, but do not begin the installation process.
3. If the passcode is recovered, do reinstall Pigeon and re-register with Signal immediately.
4. After seven full calendar days (starting from midnight at the end of the day when Pigeon was uninstalled), the linked number becomes available for a Signal registration again, for anyone who is able to receive a message to it. Install Pigeon and re-register with Signal in exactly the same way as was done originally.

5. If an attempt to re-register with Signal is made too soon, it will be necessary to wait for another seven days.

As with the initial registration, phone numbers listed in the MPO2's main Contacts list that are linked to Signal will automatically appear in the list available via 'New message'. Some will receive a 'Signal event' notification informing them that this phone number has been registered with Signal, but note that this feature can be disabled. It will again be necessary to exchange messages with people before making phone calls, and Groups will have to be rejoined by contacting members.

punkt.ch
info@punkt.ch

Tel +41 91 924 9003
Fax +41 91 924 9004

Punkt Tronics AG
Via Losanna 4
CH-6901 Lugano
Switzerland

Punkt 