DOXX DEVICE MANAGEMENT PRIVACY

What does DDM do?

DDM / MDM makes it possible for Doxx to manage (mobile) devices. In this way Doxx is able to send certain configurations to these devices. Certain settings can be set, made available and/or possibly enforced.

How DDM works?

A profile is installed on the device to be managed. This profile tells the device that it is managed by an organization and where the device should be looking for its settings / administrator (server location). When Doxx implements a configuration or setting, our server (DDM / MDM) sends a message to the Apple servers, “We have an update for device X”. The Apple server sends a message (push) to the device, “The administrator has a new configuration / setting for you”. The device knows by means of the profile where/how it needs to establish a connection with DDM in order to receive the new configuration.

When establishing a connection with DDM, the device sends/shares data. Including, for example, in the case of an iPhone, the following:

- Battery status (percentage charge)
- Name of the device
- Current provider (the name)
- Current provider network (name)
- IMEI number
- Current IP address
- Lock / lock status
- Last connection to server
- Current iOS version
- Is there a Passcode / PIN code present and does it meet the requirements?
- Phone number of the current SIM card
- Type of the iPhone
- Time zone
- List of installed applications

DDM / MDM is also able to put the phone in lost mode. The phone will then go “black” with only a message from DDM on the screen. At that moment only we (Doxx) can unlock the iPhone.
In this “lost mode”, if the device has a network connection (e.g. 4G), we can request and track its location. This mode cannot be turned on unseen and is very clear to the user.

What DDM cannot obtain?

Privacy sensitive information. DDM / MDM will never:

- Read / view messages / emails
- View photos and documents
- Track / view location (unless phone is put in lost mode)
- View user / screen (in case of iOS)

To summarize

DDM is used to manage configurations / settings on (mobile devices) with the aim of being able to “manage” the devices in accordance with the wishes / requirements of the organization / client. DDM can and will never gain access to personal and / or privacy-sensitive information on the managed device.