

BIOS unlock process for Fujitsu mobile devices

TABLE OF CONTENT

1.	Purpose of this document	1
2.	Process overview	2
3.	Proof of ownership	2
3.1.	Required information in WCM / Support Assistant	2
3.2.	Ownership acceptance	2
4.	Password removal for all devices?	3
4.1.	Customer device	3
4.2.	Company device	3
5.	Unlock process for Service Desk (1)	3
6.	Unlock process for Service Partner (2)	4
6.1.	Unlock Process for a Local Service Partner (BringIn Service Partner)	4
6.2.	Unlock Process for Onsite Service Technician	4
6.3.	Unlock process for Central Repair Centre	5
7.	Unlock Process for Chip level Repair (3)	5
7.1.	Unlock Process for Chip Level Repair (Germany, Soemmerda)	5
7.2.	Unlock Process for RLC Team (Germany, Soemmerda)	6
7.3.	Unlock Process for Remarketing & Recycling Centre (Germany, Paderborn)	6

1. Purpose of this document

Fujitsu shows a very large security and sense of responsibility towards customers.

Due to the increasing theft and data abuse, it is a matter of course that we as manufacturer offer the customer several security features. The following security features are possible: *Computrace enabled BIOS, Erase Disk, TPM, Advance Theft Protection, Hard disk password, User and supervisor BIOS and boot password, Workplace protect, smartcard and fingerprint authentication.*

In some cases it is necessary to unlock a mobile device and for such purposes Fujitsu has a special process in place to support such requests.

Caution:

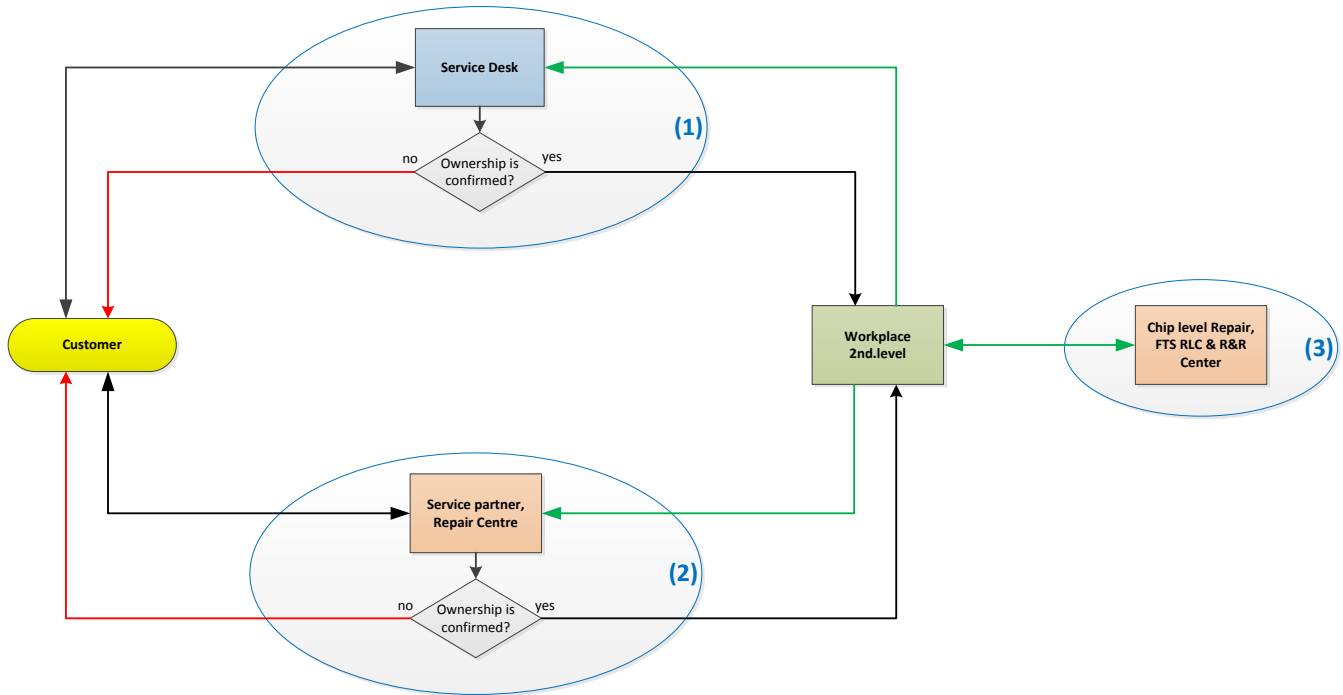
Before using the following process, it is very important to contact the customer / owner first to get the customer's approval to unlock his mobile device!

2. Process overview

According to Service Bulletin for Mobiles it is possible that Fujitsu mobile devices can be unlocked by 2nd Level Support. Please refer to current bulletin [SB-M-13012](#) located in our Extranet Portal.

To unlock Fujitsu mobile devices, three different processes are available:

- **Unlock process for Service Desk**
- **Unlock process for Service Partner (also for Onsite Technician and Central Repair Centre)**
- **Unlock process for the Chip Level Repair, Fujitsu RLC/R&R Centre**



3. Proof of ownership

3.1. Required information in WCM / Support Assistant

- a) Customer contact
- b) System type
- c) Serial number
- d) Ownership
- e) Return codes or Notebook ID (see also [SB-M-13012](#))

3.2. Ownership acceptance

The following documents will be accepted as proof of ownership:

- a) Customer invoice
- b) Customer delivery note
- c) Company delivery note
- d) Affidavit, only for device owner (template available in English and German)
- e) Confirmation of the company administrator or company IT authorized person (template available in English and German)

4. Password removal for all devices?

First, we differentiate a customer and company device.

4.1. Customer device

If the customer is the owner and buyer of this unit, then the system is a customer device. The password was set from the customer (owner) and it is possible to clear the BIOS password. Please follow the process description below. An affidavit template is also available.

4.2. Company device

A company device is a unit which is used by a company employee / customer. The owner of this device is the company. The user of this system is not its owner.

If the user does not know the BIOS password, he / she has to contact the company IT administrator. **It is not allowed to clear the password without written consent of the company, for example by the IT administrator of the company.**

If you do so, you are in violation with Fujitsu Compliance Act. The password was set by the company IT administrator according to their security policy.

To unlock a company device it is necessary to get a formless confirmation (template is available) from the company administrator. Following information is needed in this confirmation:

- Company name
- Full address of the company
- Name of the administrator or company IT authorized person
- System type
- Serial number
- Return codes / notebook ID
- Company delivery note
- Date and signature of the administrator or company IT authorized person

If all required information has been provided, please follow the process description below.

If not, then it is strictly forbidden to clear the BIOS password of the company system!

5. Unlock process for Service Desk (1)

Customer contacts Fujitsu Service Desk because of a BIOS locked Fujitsu mobile device. To get the device unlocked it is mandatory to verify ownership.

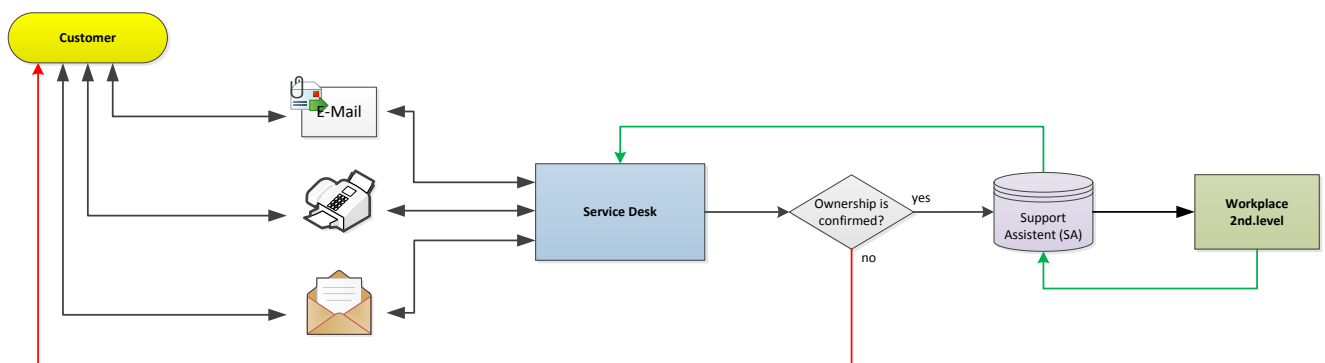
The Service Desk is responsible to check the ownership. Please note also chapter 4.2!

At first, please check the serial number in the Adler database to eliminate a potentially "stolen system". Compare the delivery notes of the customer with the entries in Adler database. If the data is not comparable, please also check the serial number in our Support Assistant (SA). Is the device recognized by the customer or company?

If yes, please forward all relevant information including customer information, proof of ownership (as attachment!), system type, serial number, return codes / notebook ID in the SA support call. Send this call to the SA *2nd Mobile* container.

The *2nd Mobile* team will verify ownership again and solve this call by generating a master password.

The Service Desk will send this master password to the customer to unlock the affected system.



6. Unlock process for Service Partner (2)

This process describes the unlock procedure for 3 different types of Service Partners:

- 6.1 Local Service Partner (BringIn Service Partner)
- 6.2 Onsite Service Partner
- 6.3 Central Repair Centre

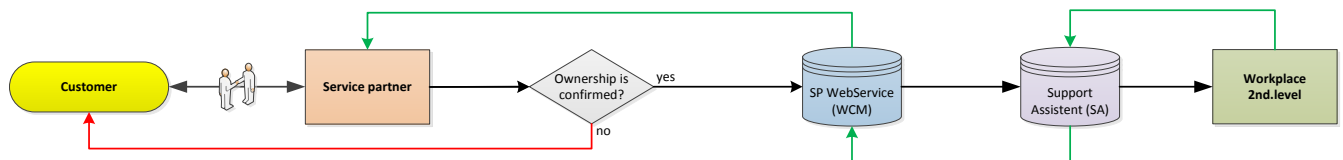
6.1. Unlock Process for a Local Service Partner (BringIn Service Partner)

Customer contacts the Fujitsu Service Partner because of repairing a device or unlocking a BIOS locked unit. For both situations, it is necessary to contact the customer first to unlock. It is forbidden to unlock a device without customers / owner's permission. If unlocking a device is requested, it is mandatory to verify the ownership.

The Service Partner is responsible for proof of ownership. Please note also chapter 4.2!

At first, please check the serial number in the Adler database to eliminate a potentially "stolen system". Compare the delivery notes of the customer with the entries in Adler database. Is the device recognized by the customer or company? Forward all relevant information like customer information with proof of ownership (as attachment!), system type, serial number, return codes or notebook ID in the WCM support call.

The *2nd Mobile* team will verify ownership again and solve this call by generating a master password. The Service Partner will unlock the affected system.



6.2. Unlock Process for Onsite Service Technician

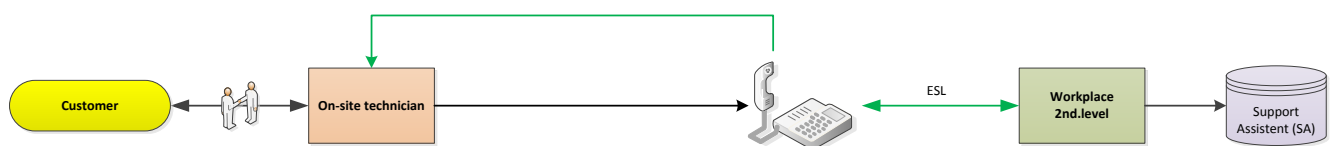
For onsite services we have two different processes:

1. Unlock process for locked delivered mainboards from Spares
2. Unlock process for locked customer device during repair

For 1:

The Onsite Service Technician contacts the Fujitsu Engineer Support Line (ESL) via phone, because of the BIOS locked delivered mainboard from Spares. The Service Partner ID, workorder number and return code or notebook ID are needed for this call.

The *2nd Mobile* team generates a Masterpassword for the Onsite Technician and creates a Support Assistant call with all information regarding this unlock call. The call can be closed afterwards.



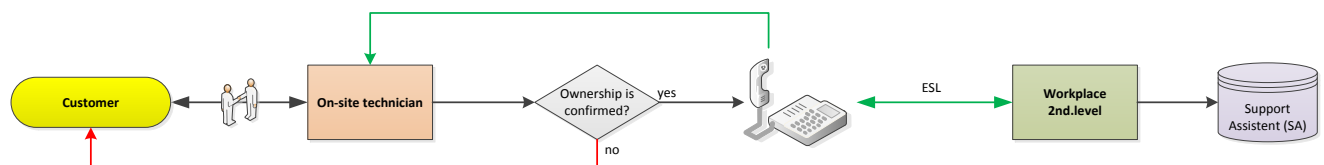
For 2:

The Onsite Service Technician is repairing a Fujitsu mobile device. For a repair it is sometimes necessary to change the settings in the BIOS setup. If the device BIOS is locked, the Onsite Technician has to ask the customer first to unlock. It is forbidden to unlock a device without customers / owners permission. If unlocking a device is requested, it is mandatory to verify the ownership.

The Onsite Technician is responsible to verified proof of ownership.

If everything was checked satisfactorily, the Service Partner contacts the Fujitsu Engineer Support Line (ESL) via phone because of the BIOS locked system. The Service Partner ID, serial number and workorder number are needed.

Next, the *2nd Mobile* team generates a Masterpassword for the Onsite Technician and creates a Support Assistant call with all information regarding this unlock call. The call can be closed afterwards.



6.3. Unlock process for Central Repair Centre

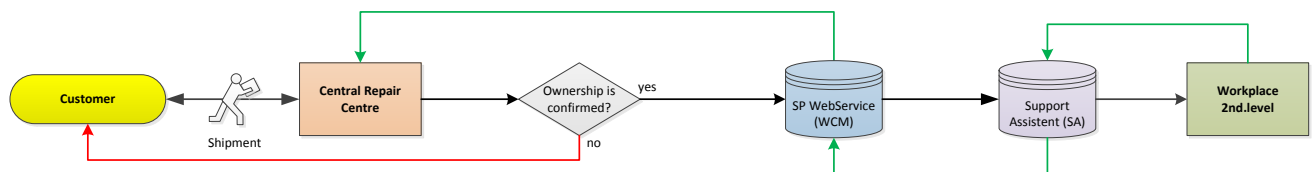
Normally, the customer does not send a locked Fujitsu device to a Central Repair Centre for unlock. In this case we recommend referring the affected customer to the local Service Desk (see above).

However, in special cases it is possible to unlock a customer BIOS locked Fujitsu device in the Central Repair Centre. During the repair process, it is necessary to contact the customer first to unlock. It is forbidden to unlock a device without customers / owners permission. If unlocking a device is requested, it is mandatory to verify the ownership.

The Repair Centre is responsible for the proof of ownership. Please note also chapter 4.2!

At first, please check the serial number in the Adler database because of a "stolen system". Compare the delivery notes of the customer with the entries in Adler database. Is the device recognized by the affected customer or company name? Forward all relevant information like customer information with proof of ownership (as attachment!), system type, serial number, return codes or notebook ID in the WCM support call.

The team of *2nd Mobile* will verify ownership again and solve this call by generating a master password. The Service Partner unlocks the affected customer device.



7. Unlock Process for Chip level Repair (3)

This process describes the unlock procedure for three different Service partners:

- 7.1 Chip Level Repair
- 7.2 Fujitsu RLC Team
- 7.3 Fujitsu R&R Centre

7.1. Unlock Process for Chip Level Repair (Germany, Soemmerda)

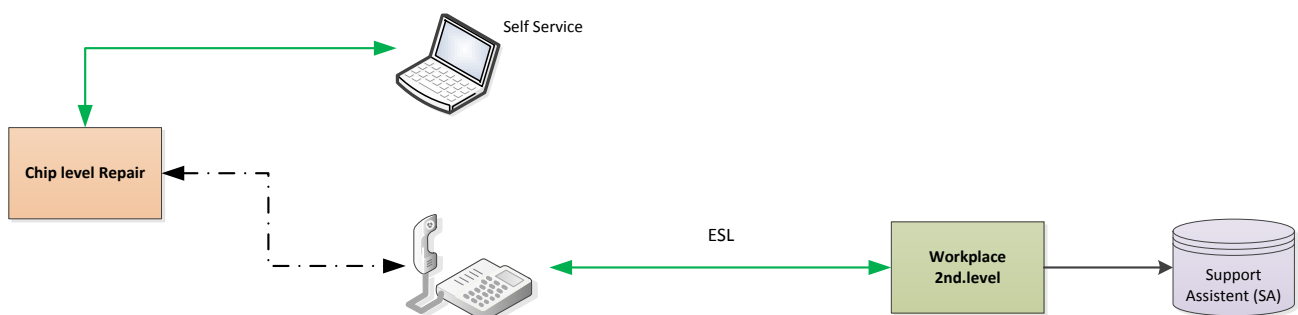
Our Chip Level Repair is located in Soemmerda and has the possibility to unlock a BIOS locked mainboard autonomously. That means, that the Chip Level Repair has the necessary unlock tools. For this unlock process it is not required to verify the ownership.

If a mainboard is not supported by the existing unlock tools, the chip level technician can contact the Engineer Support Line (ESL) via phone. The Servicepartner ID, system type and return codes or notebook ID are needed. It is also possible to attach a list of devices to this call.

The *2nd Mobile* team will then create and forward the master password via phone to the chip level technician.

The 2nd level support team will create and solve an incident in the SA database afterwards.

If needed, the tools located at Chip Level Repair will be updated by the *2nd Mobile* team.

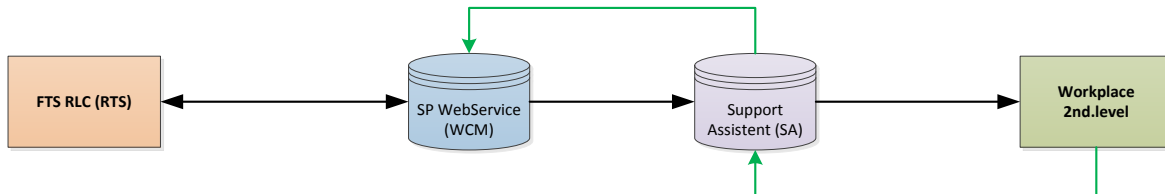


7.2. Unlock Process for RLC Team (Germany, Soemmerda)

We have a separate Service Partner located in Soemmerda reworking returned customer devices in preparation for reselling on behalf of our RLC. To unlock the system it is not mandatory to verify the ownership. This device is property of Fujitsu.

The Service Partner creates and forwards an incident in the WCM tool with system type, serial number, RMA number (10xxxxx) and return code or Notebook ID. It is also possible to attach a list of devices to this call.

The *2nd Mobile* team creates, notes the master password and solves this Incident. The Service partner unlocks the affected devices.

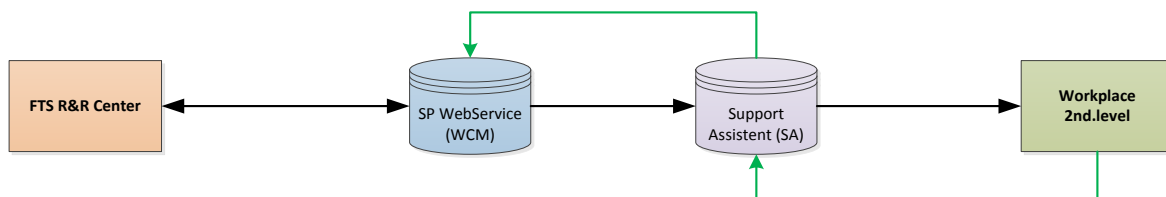


7.3. Unlock Process for Remarketing & Recycling Centre (Germany, Paderborn)

We have an own Remarketing & Recycling Centre located in Paderborn reworking returned customer devices in preparation for reselling. To unlock the system it is not mandatory to verify the ownership. This device is property of Fujitsu.

The Remarketing & Recycling Centre creates and forwards an incident in the WCM tool with system type, serial number, Remarketing & Recycling ID ("RR-84W01") and return code or Notebook ID. It is also possible to attach a list of devices to this call.

The *2nd Mobile* team creates, notes the master password and solves this Incident. The Fujitsu R&R Centre unlocks the affected devices.



PUBLISHED BY DEPARTMENT

Fujitsu EMEA
Solutions & Technical Support
E-mail: technical.support@ts.fujitsu.com
Internet: <https://ts.fujitsu.com/support>

PARTNER LOGIN

partners.ts.fujitsu.com

All rights reserved, including intellectual property rights. Technical data subject to modifications and delivery subject to availability. Any liability that the data and illustrations are complete, actual or correct is excluded. Designations may be trademarks and/or copyrights of the respective manufacturer, the use of which by third parties for their own purposes may infringe the rights of such owner. For further information see ts.fujitsu.com/terms_of_use.html

Copyright © Fujitsu Technology Solutions GmbH 2015