



## **UHF RFID Passwords and Locks**

iDTRONIC GmbH  
Donnersbergweg 1  
67059 Ludwigshafen  
Germany/Deutschland

Phone: +49 621 6690094-0  
Fax: +49 621 6690094-9  
E-Mail: [info@idtronic.de](mailto:info@idtronic.de)  
Web: [idtronic.de](http://idtronic.de)

Issue 0.2  
– 23. March 2017 –

Subject to alteration without prior notice.  
© Copyright iDTRONIC GmbH 2016  
Printed in Germany

## Contents

<b>1</b>	<b>Memory Types on The RFID Tag .....</b>	<b>4</b>
1.1	Reserved Memory.....	4
1.2	EPC Memory .....	4
1.3	TID Memory .....	4
1.4	User Memory .....	4
1.5	Chart of Memory Bank Layout.....	4
<b>2</b>	<b>Locks .....</b>	<b>4</b>
2.1	Important Note.....	4
2.2	Set Password Protection.....	4
2.3	Security of Lock Status.....	5
2.4	Possible Locks of Memory Banks EPC, TID, User .....	5
2.5	Possible Locks of Password in Reserved Memory .....	5
<b>3</b>	<b>Setting Access Restrictions with the Reader Demo Tool.....</b>	<b>6</b>
3.1	Set Password .....	6
3.2	Set Locks .....	7

## 1 Memory Types on The RFID Tag

### 1.1 Reserved Memory

This memory bank is 8 Byte (= 16 nibbles = 64 bit in size. The first 4 Bytes (blocks 0 & 1) contain the KILL password, and the following 4 Bytes (blocks 2 & 3) the ACCESS password. After you have written a password, this memory bank should be locked, so the passwords cannot be easily read out and overwritten (pls. see below).

### 1.2 EPC Memory

This memory bank contains the EPC (electronic product code) and further bytes (PC – Protocol Control, CRC – Checksum of EPC). It is at least 12 Bytes = 24 nibbles = 96 bits in size. Some RFID tag types can allocate bytes from the user memory bank to the EPC memory bank, so larger EPCs can be stored.

Minimum size: 2 bytes CRC + 2 Bytes PC + 12 Bytes EPC

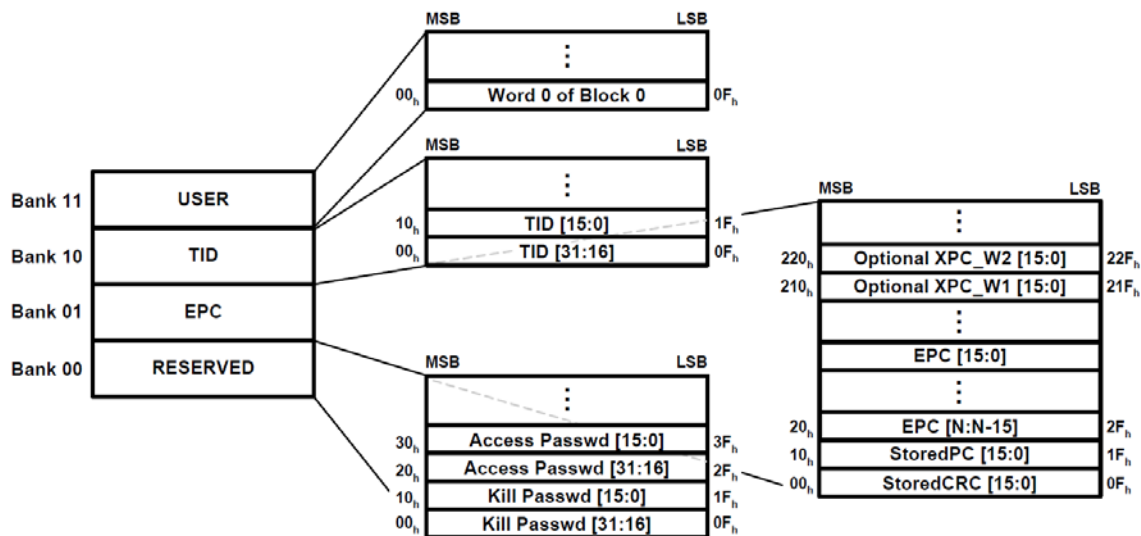
### 1.3 TID Memory

This unique tag ID is written in chip factory and can typically not be altered.

### 1.4 User Memory

The user memory is not available for all types of RFID tag types. Some have only 64 bytes (= 128 nibbles = 512 bits). There are also RFID tag types with up to 8 kbytes of memory.

### 1.5 Chart of Memory Bank Layout



## 2 Locks

### 2.1 Important Note

Only reserved memory bank (access and kill passwords) can be both write and READ locked—all others (EPC, TID, and User) can be write-locked only. Typically the Tag Identification (TID) memory bank is perma-locked at the chip factory.

### 2.2 Set Password Protection

1. Write password into reserved memory bank.
2. Lock access password.

3. Lock the desired memory bank (EPC or User) against changes (write lock memory bank).

If the access password is not locked, the password can simply be read from the reserved memory bank and used. Unless they were permanently locked (perma-locked, always not writable / accessible).

### 2.3 Security of Lock Status

The lock status cannot be retrieved from the tag, it can only be altered. It can only be detected by error messages when access to locked functions is performed.

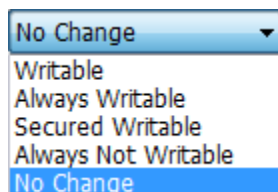
### 2.4 Possible Locks of Memory Banks EPC, TID, User

These memory banks are always readable. They can only be locked against alteration.

**There are these 4 lock states:**

1. Unlocked and writable.
2. Perma-UNlocked and always writable (can never be locked).
3. Locked, locked, secured writable with password.
4. Perma-locked, memory content can no longer be altered (can never be unlocked, always not writable).

**Selection in BLUEBOX Show**



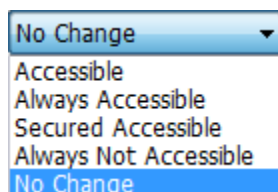
### 2.5 Possible Locks of Password in Reserved Memory

This memory bank can also be disabled against read-out. The access password can be blocked separately from the kill password.

**There are these 4 lock states:**

1. Unlocked and fully accessible (read + write).
2. Perma-UNlocked, can never be locked, always accessible (read + write).
3. locked, secured accessible with password (read + write).
4. Perma-locked, can never be unlocked, always not accessible

**Selection in BLUEBOX Show**



### 3 Setting Access Restrictions with the Reader Demo Tool

**Gen2 - Tag Settings**

EPC: **00-00-00-18-83-10-00-28-15-20-78-88**

Reader Id: **PUR RM1 - 00-00-23-a0 @ \\.\COM15**

Information

Manufacturer: **Alien Technology** Refresh

Model Number: **0x000412**

User Memory Size: **-**

Functions

Read / Write Set EPC Text Edit

**Set Password** **Lock** Kill

#### 3.1 Set Password

**Gen2 - Set Password**

EPC **00-00-00-18-83-10-00-28-15-20-78-88**

Current Access Password: **00-00-00-00**

Password Type: **Access**

New Password: **00-00-00-00**

Ok Cancel

Select which password to set:

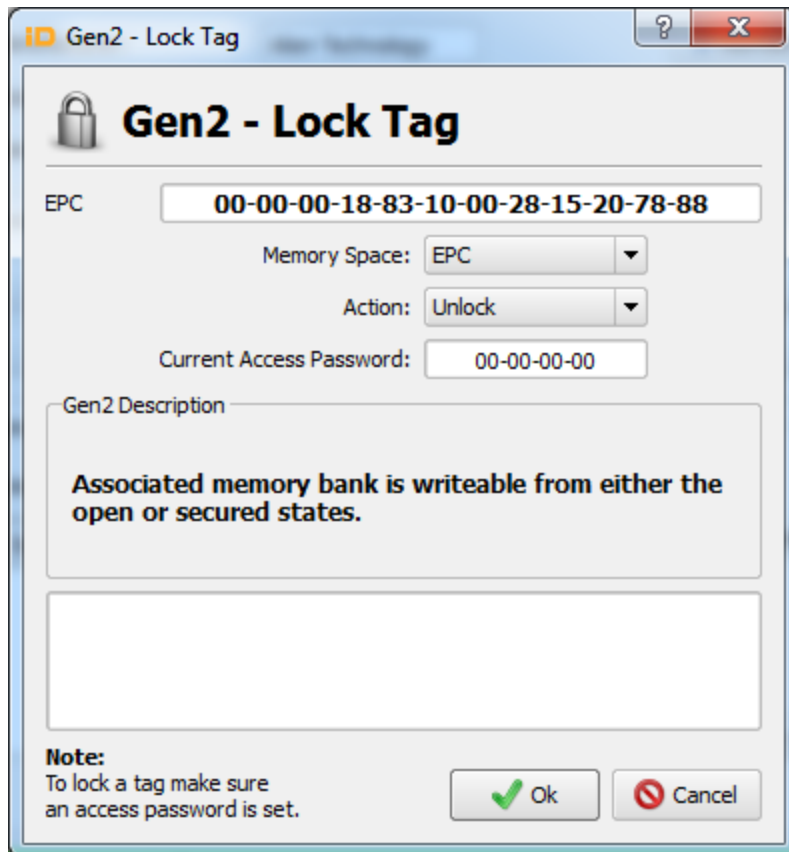
EPC **00-00-00-18-83-10-00-28-15-20-78-88**

Current Access Password: **00-00-00-00**

Password Type: **Access**

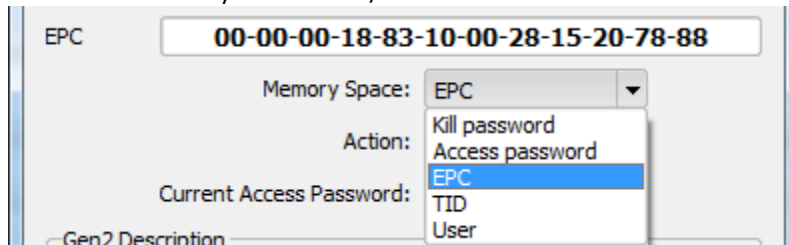
New Password: **Access**

### 3.2 Set Locks



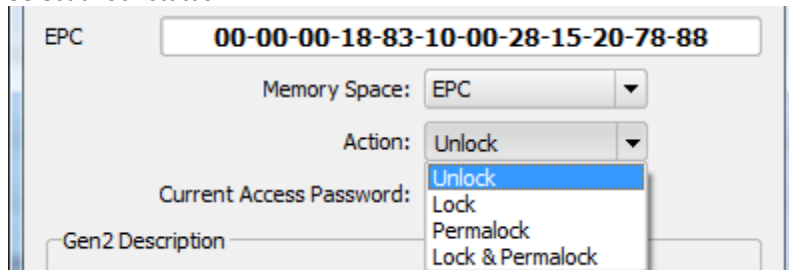
The screenshot shows the 'Gen2 - Lock Tag' dialog box. It features a title bar with a question mark and a close button. The main area has a lock icon and the title 'Gen2 - Lock Tag'. Below this, there is an 'EPC' field with the value '00-00-00-18-83-10-00-28-15-20-78-88'. A 'Memory Space' dropdown menu is set to 'EPC'. An 'Action' dropdown menu is set to 'Unlock'. A 'Current Access Password' field contains '00-00-00-00'. A 'Gen2 Description' text box contains the text: 'Associated memory bank is writeable from either the open or secured states.' At the bottom, there is a 'Note' section with the text: 'To lock a tag make sure an access password is set.' and two buttons: 'Ok' (with a green checkmark) and 'Cancel' (with a red X).

Select what memory bank to lock/unlock:



This screenshot shows the 'Gen2 - Lock Tag' dialog box with the 'Action' dropdown menu open. The menu options are: 'Kill password', 'Access password', 'EPC' (highlighted in blue), 'TID', and 'User'. The other fields and the 'Gen2 Description' text box remain the same as in the previous screenshot.

Select a lock status:



This screenshot shows the 'Gen2 - Lock Tag' dialog box with the 'Action' dropdown menu open. The menu options are: 'Unlock' (highlighted in blue), 'Lock', 'Permalock', and 'Lock & Permalock'. The other fields and the 'Gen2 Description' text box remain the same as in the previous screenshot.



## **UHF RFID Passwörter und Sperren**



iDTRONIC GmbH  
Donnersbergweg 1  
67059 Ludwigshafen  
Germany/Deutschland

Ausgabe 0.2  
– 23. März 2017 –

Telefon: +49 621 6690094-0  
Fax: +49 621 6690094-9  
E-Mail: [info@idtronic.de](mailto:info@idtronic.de)  
Web: [idtronic.de](http://idtronic.de)

Änderungen ohne vorherige Ankündigung vorbehalten.  
© Copyright iDTRONIC GmbH 2016  
Printed in Germany

## Inhalt

<b>1</b>	<b>Speichertypen auf dem RFID-Datenträger .....</b>	<b>4</b>
1.1	Reserved Memory.....	4
1.2	EPC Memory .....	4
1.3	TID Memory .....	4
1.4	User Memory .....	4
1.5	Schaubild der Speicherbänke.....	4
<b>2</b>	<b>Sperren .....</b>	<b>4</b>
2.1	Wichtiger Hinweis.....	4
2.2	Passwortschutz einstellen.....	5
2.3	Sicherheit des Sperrzustandes .....	5
2.4	Mögliche Sperren der Speicherbänke EPC, TID, User .....	5
2.5	Mögliche Sperren der Passwörter in Reserved Memory .....	5
<b>3</b>	<b>Sperren mit dem Reader Demo Tool .....</b>	<b>6</b>
3.1	Passwort setzen .....	6
3.2	Sperren setzen .....	7

## 1 Speichertypen auf dem RFID-Datenträger

### 1.1 Reserved Memory

Diese Speicherbank ist 8 Byte (= 16 nibbles = 64 bit) groß. Sie enthält in den ersten 4 Byte (Blöcke 0 & 1) das KILL-Passwort und in den weiteren 4 Byte (Blöcke 2 & 3) das Zugriffspasswort (ACCESS Passwort). Wenn sie ein Passwort geschrieben haben, sollten Sie diese Speicherbank sperren (lock), damit die Passwörter nicht einfach ausgelesen und überschrieben werden können (siehe im Folgenden).

### 1.2 EPC Memory

Diese Speicherbank enthält den EPC (Elektronischer Produkt-Code) und weitere Zusatzbytes (PC – Protocol Control, CRC – Prüfsumme des EPCs). Sie ist mindestens 12 Byte = 24 nibble = 96 bit groß. Manche RFID-Datenträgertypen können vom Benutzerspeicher (User Memory) Bytes abzwacken und der EPC-Speicherbank zuweisen, so dass ein längerer EPC gespeichert werden kann.

Mindestgröße: 2 Byte CRC + 2 Byte PC + 12 Byte EPC

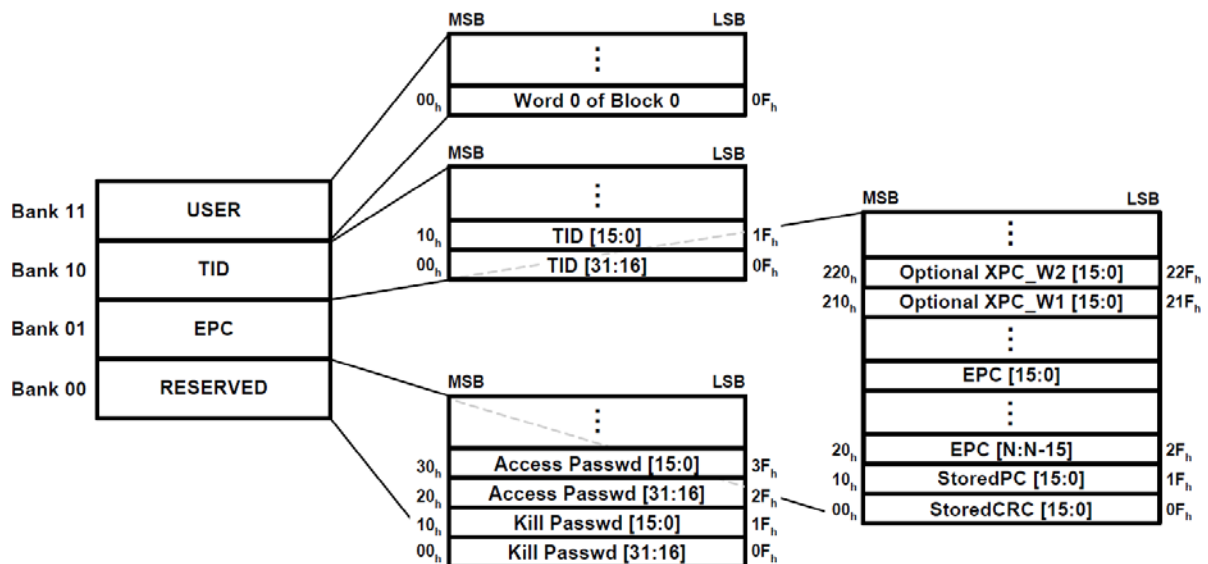
### 1.3 TID Memory

Diese eindeutige Tag-ID wird vom Chiphersteller geschrieben und kann im Allgemeinen nicht verändert werden.

### 1.4 User Memory

Der Benutzerspeicher steht nicht bei allen RFID-Datenträger-Typen zur Verfügung. Manche haben nur 64 Byte (= 128 nibbles = 512 bit). Es gibt auch RFID-Datenträger-Typen mit bis zu 8 kByte Speicherplatz.

### 1.5 Schaubild der Speicherbänke



## 2 Sperren

### 2.1 Wichtiger Hinweis

Nur die Speicherbank Reserved Memory kann gegen Schreiben UND Lesen gesperrt werden. Alle anderen Speicherbänke sind immer lesbar. Die TID-Speicherbank ist üblicherweise vom Chiphersteller aus dauerhaft gegen Schreiben gesperrt (perma-locked).

## 2.2 Passwortschutz einstellen

1. Schreiben Sie das Passwort in die Speicherbank Reserved Memory.
2. Sperren Sie das Zugriffspasswort (lock access password).
3. Sperren Sie die gewünschte Speicherbank (EPC oder User) gegen Änderungen (lock memory bank).

Wird das Zugriffspasswort nicht gesperrt, kann das Passwort einfach aus der Speicherbank Reserved Memory ausgelesen und verwendet werden. Es sei denn, sie wurden dauerhaft gesperrt (perma-locked, always not writable/accessible).

## 2.3 Sicherheit des Sperrzustandes

Der Sperrzustand (Lock status) kann nicht abgefragt werden, er kann nur verändert werden. Herausfinden kann man ihn nur anhand von Fehlermeldungen, wenn gesperrte Zugriffe (Schreiben oder Lesen) ausgeführt werden.

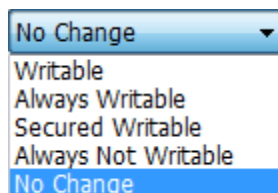
## 2.4 Mögliche Sperren der Speicherbänke EPC, TID, User

Diese Speicherbänke sind immer lesbar. Sie können nur gegen Veränderung gesperrt werden.

### Es gibt diese 4 Sperrzustände

1. Ungesperrt und beschreibbar (unlocked, writable)
2. Dauerhaft ungesperrt und beschreibbar (can never be locked, always writable)
3. Gesperrt, kann nur mit Passwort beschrieben werden (locked, secured writable)
4. Dauerhaft gesperrt, der Speicherinhalt kann nicht mehr verändert werden (perma-locked, can never be unlocked, always not writable)

### Auswahl in BLUEBOX Show



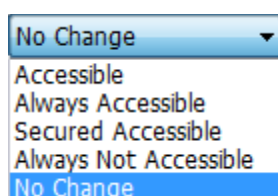
## 2.5 Mögliche Sperren der Passwörter in Reserved Memory

Diese Speicherbank kann auch gegen Auslesen gesperrt werden. Dabei kann das Zugriffspasswort (Access Code) getrennt vom Abschaltpasswort (Kill Code) gesperrt werden.

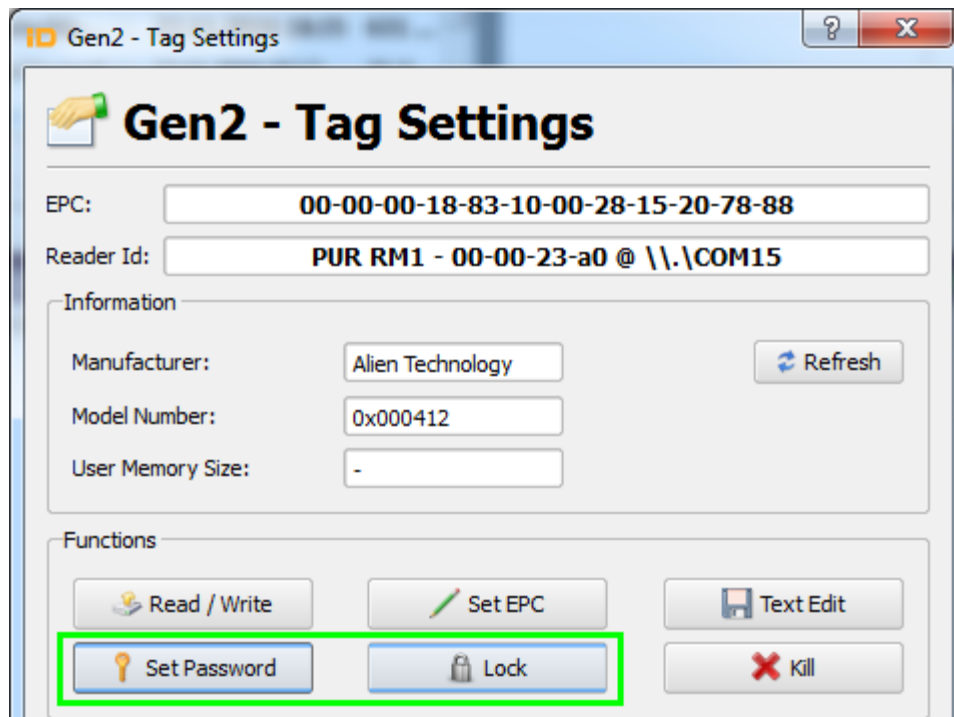
### Es gibt diese 4 Sperrzustände

1. Ungesperrt, lesbar und beschreibbar (unlocked, accessible)
2. Dauerhaft ungesperrt, lesbar und beschreibbar (perma-unlocked, can never be locked, always accessible)
3. Nur mit Passwort lesbar und beschreibbar (locked, secured accessible)
4. Überhaupt nicht lesbar und beschreibbar (perma-locked, can never be unlocked, always not accessible)

### Auswahl in BLUEBOX Show



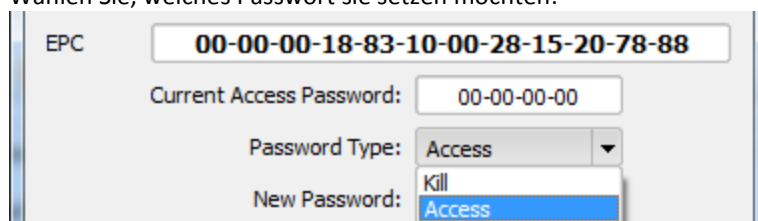
### 3 Sperren mit dem Reader Demo Tool



#### 3.1 Passwort setzen



Wählen Sie, welches Passwort sie setzen möchten:



### 3.2 Sperren setzen



**Gen2 - Lock Tag**

EPC: **00-00-00-18-83-10-00-28-15-20-78-88**

Memory Space: **EPC**

Action: **Unlock**

Current Access Password: **00-00-00-00**

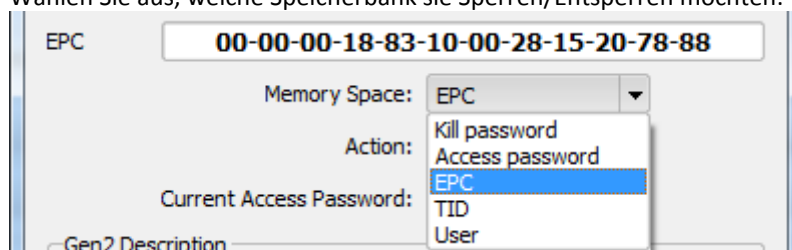
Gen2 Description:

**Associated memory bank is writeable from either the open or secured states.**

**Note:**  
To lock a tag make sure an access password is set.

**Ok** **Cancel**

Wählen Sie aus, welche Speicherbank sie Sperren/Entsperren möchten:



EPC: **00-00-00-18-83-10-00-28-15-20-78-88**

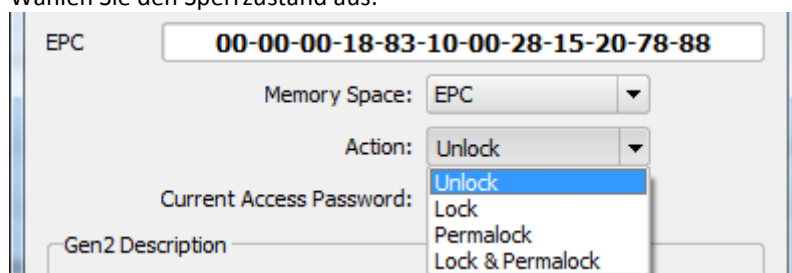
Memory Space: **EPC**

Action: **EPC**

Current Access Password:

Gen2 Description:

Wählen Sie den Sperrzustand aus:



EPC: **00-00-00-18-83-10-00-28-15-20-78-88**

Memory Space: **EPC**

Action: **Unlock**

Current Access Password:

Gen2 Description: