MAGENSA™
SIMPLY STOPS FRAUD

MICRSAFE

Remote Services

Reference Manual

November 2014

Manual Part Number:
D998200025 rev1.0

REGISTERED TO ISO 9001:2008

Table 0.1 - Revisions

Rev Number	Date	Notes
1.01	**November 2014**	Initial Release

Table of Contents

Table 0.1 - Revisions 2

Table of Contents 3

CERTIFICATION 4

MagTek is an official ESO 4

1. COMPUTER/BROWSER CONFIGURATION 5

2. CONNECTING 6

USB DRIVER INSTALLATION (WINDOWS) 6

REMOTE SERVICES INSTALLER 6

2. CHANGE SECURITY LEVEL 7

3. KEY LOAD 9

3. MASKING 11

4. AAMVA MASKING 13

CERTIFICATION

MagTek is an official ESO

MagTek®'s secure infrastructure allows users to safely and remotely configure devices and inject encryption keys while minimizing risk, lowering costs and enhancing overall operations.

MagTek is an official ESO (Encryption Support Organization). For more details on MagTek and Magensa's PCI-DSS or ESO status, visit VISA's Global Registry of Service Providers.

Go to www.visa.com/splisting/.
Press Begin Search.
Type in “Magensa” under Company Name. (To confirm PCI-DSS and ESO).
Type in “MagTek” under Company Name.   (To confirm TPA and ESO).
Press GO.
Magensa PCI and ESO certifications will appear.

1. COMPUTER/BROWSER CONFIGURATION

Before the user begins, please make sure the following steps have been sucessfully completed. Upon success, the user will be able to connect to Magensa's Remote Services for MICRSafe.

1. Open a browser on the computer.
    a. Make sure to choose 'Run as administrator' when opening the browser
        i. Internet Explorer, Firefox and Chrome are recommended
2. Update/Confirm the computer has latest version of Java installed.
    a. Go to http://java.com/en/download/index.jsp

2. CONNECTING

The following is required for the Installation of the MICRSafe:

1. Connect USB cable, Part Number 22553301 to the MICRSafe
1. Connect the DC Power Adapter with Cable, 120VAC to 12 VDC, 1 Amp, Part Number 64300118 to the MICRSafe (64300121 for international customers)
2. Connect the interface cable's USB A connector to the PC
3. Connect the DC power adapter's plug to the wall outlet
4. The LED indicator on the MICRSafe should turn on to a steady green. The LED indicator is located to the left of the slot where the check is first inserted for reading.

USB DRIVER INSTALLATION (WINDOWS)

On hosts with the Windows operating system, the first time the MICRSafe is plugged into a specific USB port, Windows will open a dialog box which will guide you through the process of installing a driver for the device; follow the instructions given in the dialog box. Windows will install the driver that is used for HID keyboard devices; this driver is a basic component of all modern versions of the Windows operating system.

REMOTE SERVICES INSTALLER

1. Using the browser, navigate to https://rs.magensa.net/rs/controls/99510133.exe
    a. Make sure to choose 'Run as administrator' when opening the browser

2. *This is to download and run INSTALLER
    a. Click Enter
    b. Click Run
    c. Answer Yes to Pop-ups
    d. Click Install
    e. Click Finish

The computer should now be ready to use Magensa's Remote Services

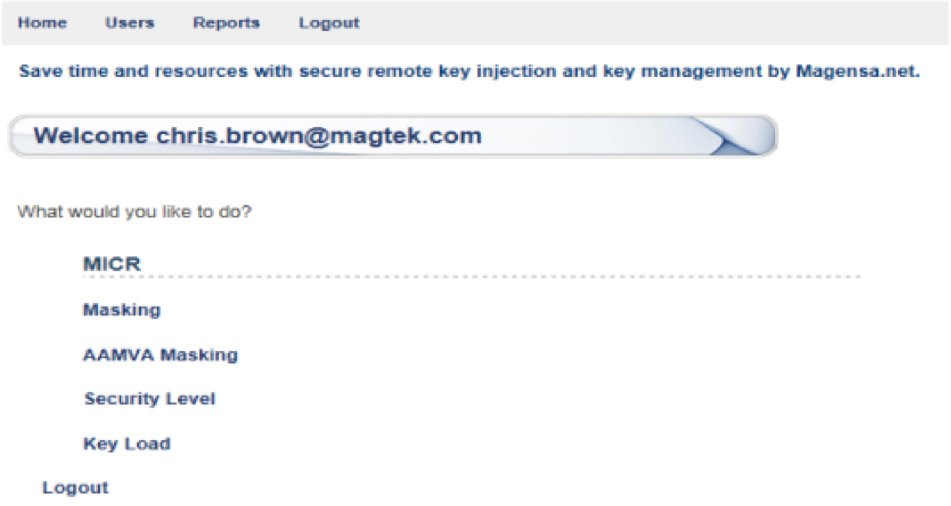
Caution

Do not place the MICRSafe within 6 inches of a computer monitor or power supply. These devices may cause undesirable interference with the check reading operation.

2. CHANGE SECURITY LEVEL

The MICRSafe may have been deployed in security Level 2 which allows clear-text magstripe and MICR data to transmit from the MICRSafe. The user may choose to change the Security Level to 3 whereby the magstripe and MICR data will be encrypted using 3DES encryption and DUKPT key management. Follow the steps below to ensure the MICRSafe is configured to allow for subsequent Key Loading and Masking options to be changed.

Step 1: From the MENU page, Click Security Level

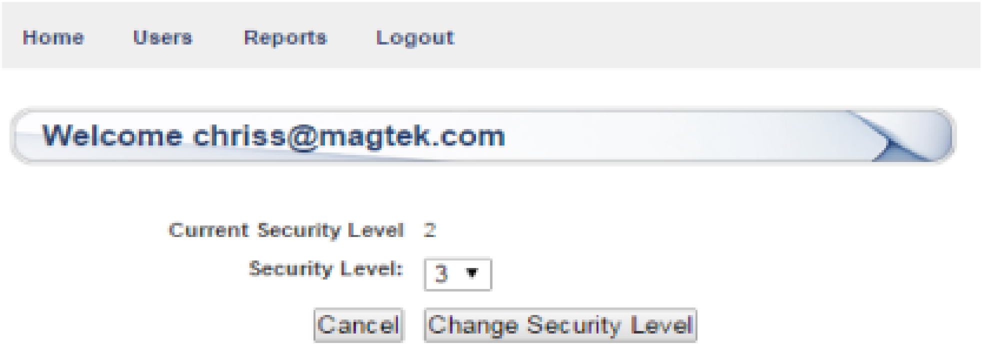


Save time and resources with secure remote key injection and key management by Magensa.net.

Welcome chris.brown@magtek.com

What would you like to do?

Step 2: To change from Security Level 2 to Security Level 3, select 3 from the drop-down menu, then click Change Security Level.



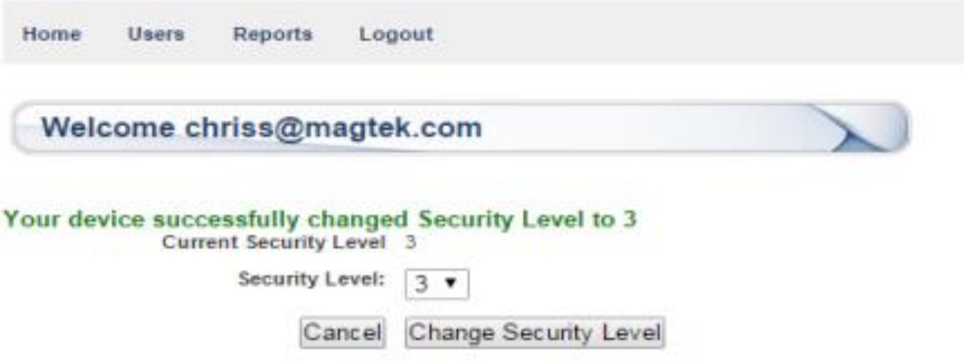
Welcome chriss@magtek.com

Current Security Level 2

Security Level: 3 ▼

After a few seconds, a message will display indicating the outcome such as “Your device successfully changed Security Level to 3”

2. CHANGE SECURITY LEVEL



Welcome chriss@magtek.com

Your device successfully changed Security Level to 3

Current Security Level 3

Security Level: 3 ▾

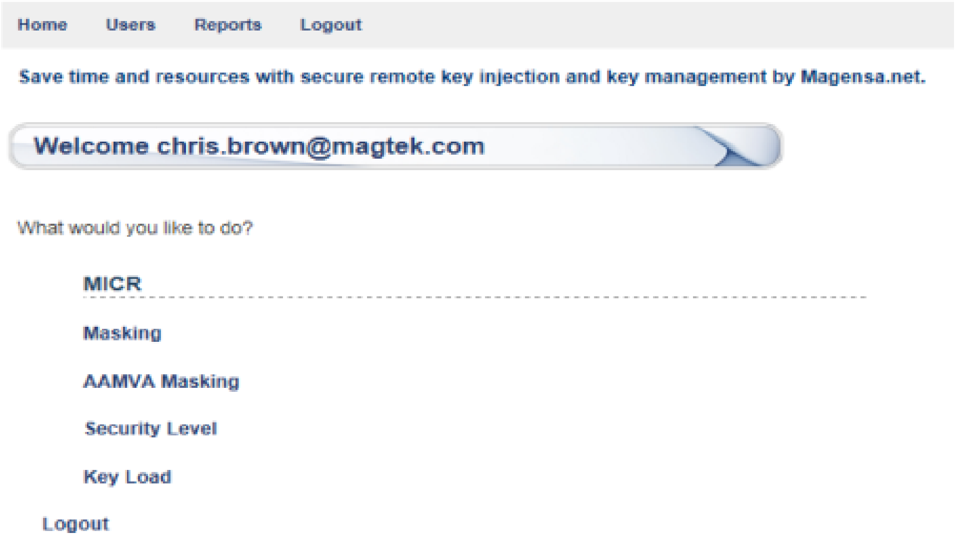
Security Level Options:

- The ONLY option supported for changing Security Level is Security Level 3. Once a MICRSafe has been promoted to Security Level 3, the MICRSafe will not be able to revert to Security Level 2.

3. KEY LOAD

The MICRSafe may have been deployed with certain Production Key that the user wishes to change. To change the encryption key, the MICRSafe MUST be in Security Level 3. Follow the steps below to change encryption keys.

Step 1: On the MENU page, click Key Load

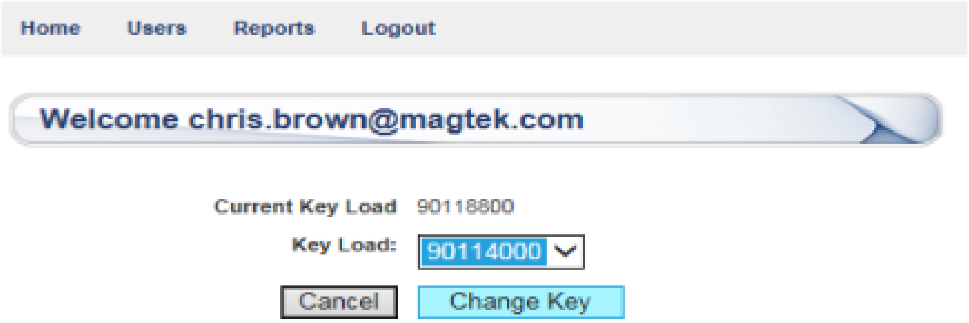


Save time and resources with secure remote key injection and key management by Magensa.net.

Welcome chris.brown@magtek.com

What would you like to do?

Step 2: Select a Key to load from the drop-down menu, then click Change Key



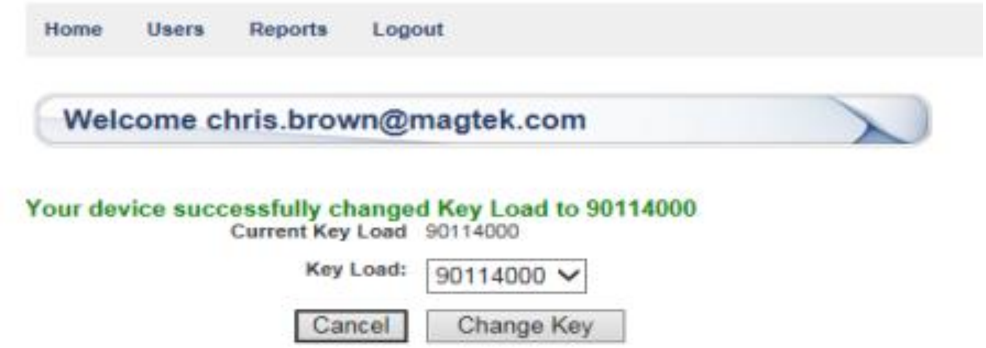
Welcome chris.brown@magtek.com

Current Key Load 90118800

Key Load: 90114000

3. KEY LOAD

After a few seconds, a message will display indicating the outcome such as “Your device successfully changed Key Load to [insert key identifier here]”



Your device successfully changed Key Load to 90114000

Current Key Load 90114000

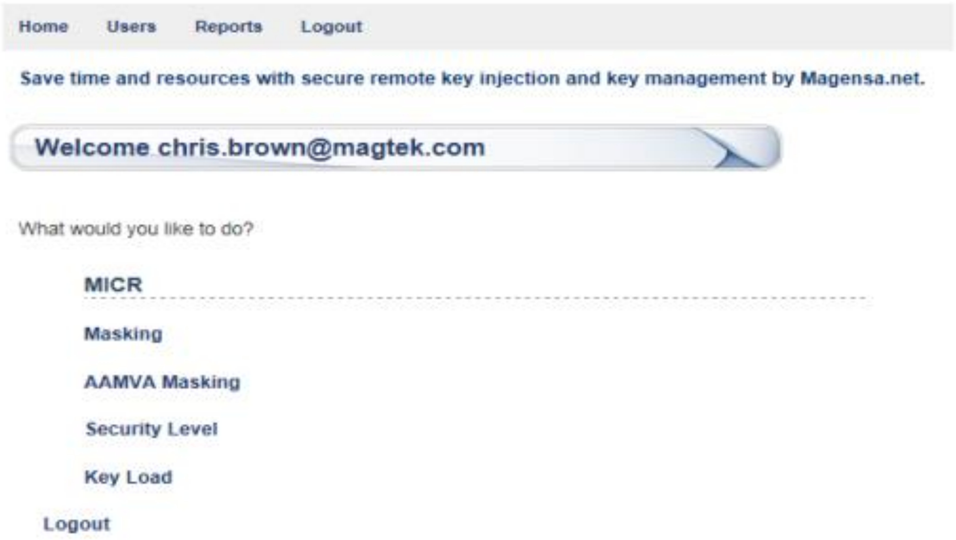
Key Load: 90114000

Key Load Options:
The encryption keys available for Key Loading are controlled by Magensa and configured for access based on a user’s profile. The keys available will be displayed as the KSN or Key Serial Number.

3. MASKING

When the MICRSafe is configured for Security Level 3, the magstripe and MICR data will be fully encrypted. However, certain magstripe data elements that are considered non-sensitive can be exposed or un-masked in clear-text. The Masking option allows the user to determine which data elements to expose. To change Masking options, the MICRSafe MUST be in Security Level 3. Follow the steps below to configure the desired Masking.

Step 1: On the MENU page, Click Masking

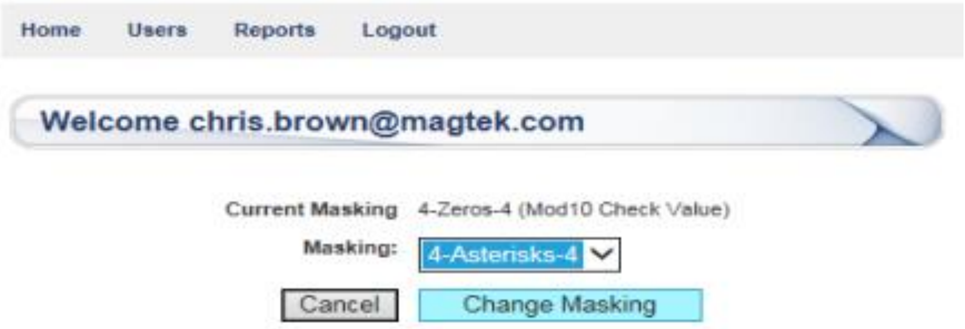


Save time and resources with secure remote key injection and key management by Magensa.net.

Welcome chris.brown@magtek.com

What would you like to do?

Step 2: Select a Masking option from the drop-down menu, then click Change Masking

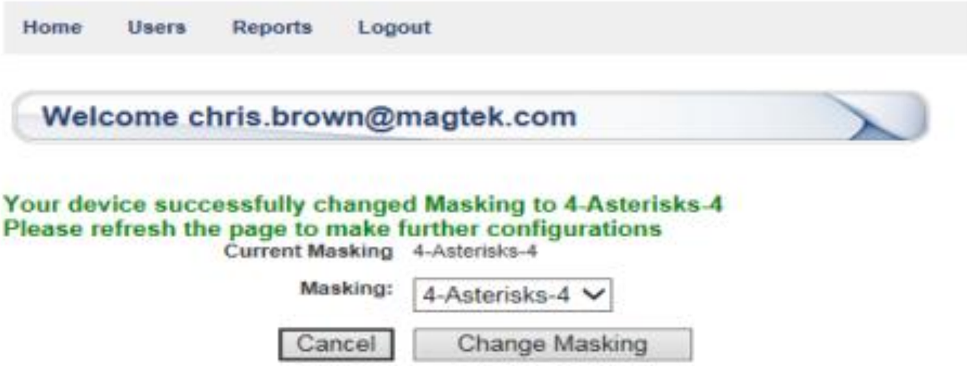


Welcome chris.brown@magtek.com

Current Masking 4-Zeros-4 (Mod10 Check Value)

Masking: 4-Asterisks-4

After a few seconds, a message will display indicating the outcome such as "Your device successfully changed Masking to 4-Asterisks-4"



Your device successfully changed Masking to 4-Asterisks-4
Please refresh the page to make further configurations

Current Masking 4-Asterisks-4

Masking: 4-Asterisks-4

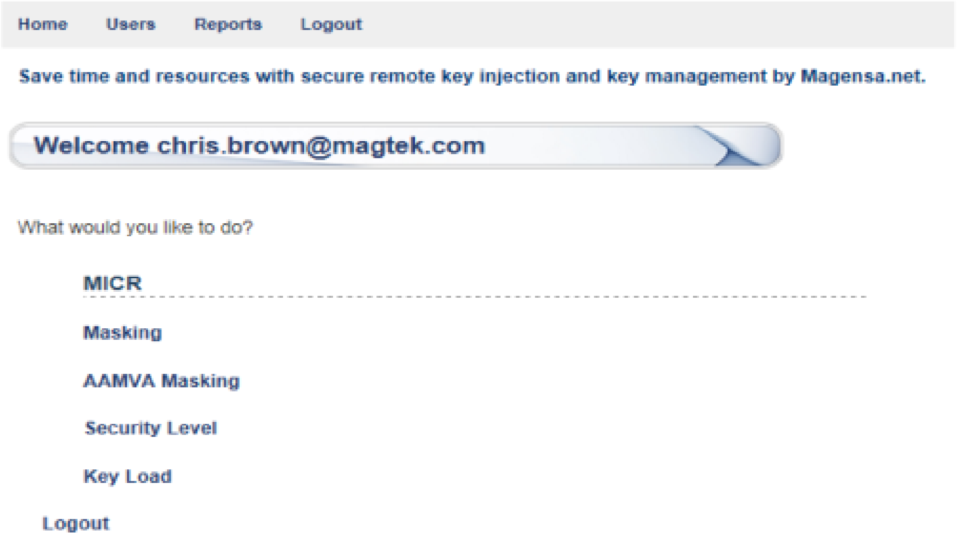
Masking Options:

- 4-Asterisks-4 means the first 4 and last digits of the cardholder's primary account number will be exposed in clear-text. The middle digits will be obfuscated with asterisks.
- 4-Zeros-4 (No Mod 10) means the first 4 and last digits of the cardholder's primary account number will be exposed in clear-text. The middle digits will be obfuscated with zeros. A MOD 10 check digit will not be used.
- 4-Zeros-4 (with Mod 10) means the first 4 and last digits of the cardholder's primary account number will be exposed in clear-text. The middle digits will be obfuscated with zeros. A MOD 10 check digit will be used.
- 6-Asterisks-4
- 6-Zeros-4 (No Mod 10) means the first 6 and last digits of the cardholder's primary account number will be exposed in clear-text. The middle digits will be obfuscated with zeros. A MOD 10 check digit will not be used.
- 6-Zeros-4 (with Mod 10) means the first 6 and last digits of the cardholder's primary account number will be exposed in clear-text. The middle digits will be obfuscated with zeros. A MOD 10 check digit will be used.

4. AAMVA MASKING

When the MICRSafe is configured for Security Level 3, the magstripe and MICR data will be fully encrypted. However, the user may wish to read AAMVA encoded Driver's Licenses and expose certain data elements that are considered non-sensitive. The AAMVA Masking option allows the user to determine which data elements to expose when reading an AAMVA encoded Driver's License. To change AAMVA Masking options, the MICRSafe MUST be in Security Level 3. Follow the steps below to configure the desired AAMVA Masking.

Step 1: On the MENU page, Click AAMVA Masking

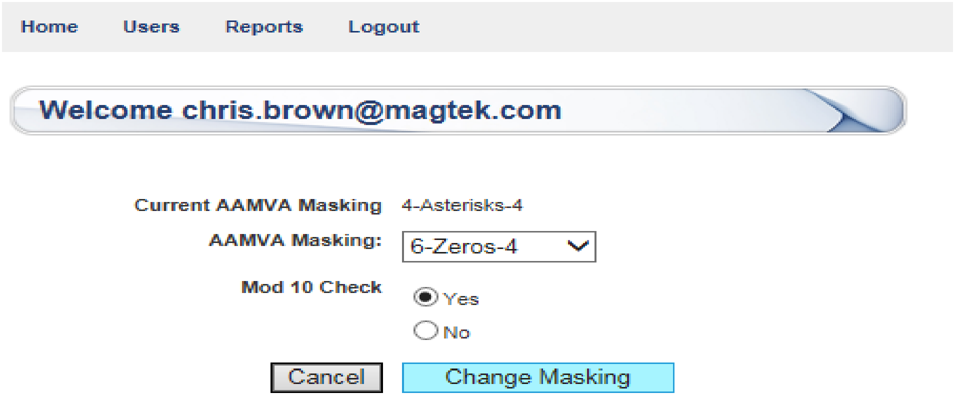


Save time and resources with secure remote key injection and key management by Magensa.net.

Welcome chris.brown@magtek.com

What would you like to do?

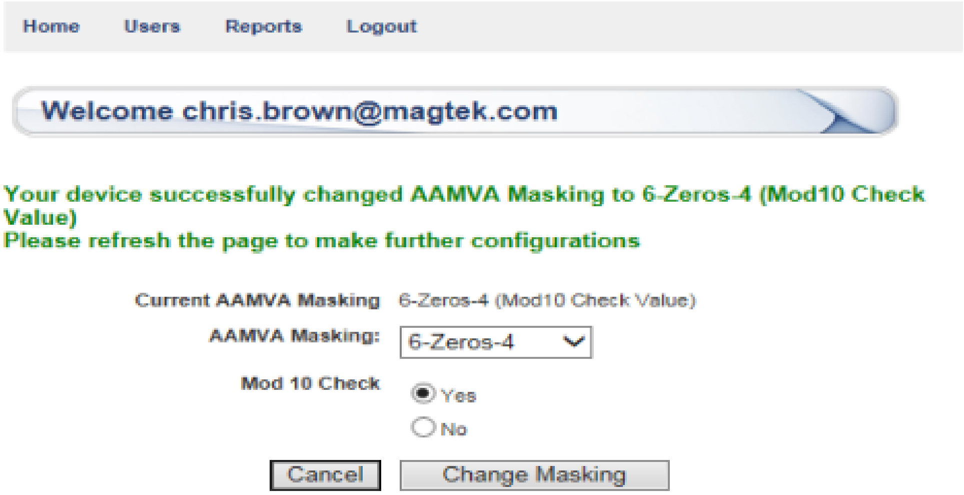
Step 2: Select an AAMVA Masking option from the drop-down menu, then click Change Masking



Welcome chris.brown@magtek.com

Current AAMVA Masking	4-Asterisks-4
AAMVA Masking:	6-Zeros-4
Mod 10 Check	● Yes ○ No

After a few seconds, a message will display indicating the outcome such as "Your device successfully changed AAMVA Masking to 6-Zeros-4 (Mod10 Check Value)"



Welcome chris.brown@magtek.com

Your device successfully changed AAMVA Masking to 6-Zeros-4 (Mod10 Check Value)
Please refresh the page to make further configurations

Current AAMVA Masking 6-Zeros-4 (Mod10 Check Value)

AAMVA Masking: 6-Zeros-4

Mod 10 Check ● Yes ○ No

AAMVA Masking Options:

- 4-Asterisks-4 means the first 4 and last digits of the cardholder's primary account number from an AAMVA Driver's License will be exposed in clear-text. The middle digits will be obfuscated with asterisks.
- 4-Zeros-4 (No Mod 10) means the first 4 and last digits of the cardholder's primary account number from an AAMVA Driver's License will be exposed in clear-text. The middle digits will be obfuscated with zeros. A MOD 10 check digit will not be used.
- 4-Zeros-4 (with Mod 10) means the first 4 and last digits of the cardholder's primary account number from an AAMVA Driver's License will be exposed in clear-text. The middle digits will be obfuscated with zeros. A MOD 10 check digit will be used.
- 6-Asterisks-4
- 6-Zeros-4 (No Mod 10) means the first 6 and last digits of the cardholder's primary account number from an AAMVA Driver's License will be exposed in clear-text. The middle digits will be obfuscated with zeros. A MOD 10 check digit will not be used.
- 6-Zeros-4 (with Mod 10) means the first 6 and last digits of the cardholder's primary account number from an AAMVA Driver's License will be exposed in clear-text. The middle digits will be obfuscated with zeros. A MOD 10 check digit will be used
- Unmasked means the entire Track 2 of an AAMVA Driver's License will be exposed in clear-text. Track 1 and 3 (if present) will remain fully encrypted.