**Magento Stages of Authentication**

**Dynamic Factor Authentication**

<table>
<thead>
<tr>
<th>Topology Key</th>
<th>Stage 1</th>
<th>Stage 2</th>
<th>Stage 3</th>
<th>Stage 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User time</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCRA hardware token</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User card swipe</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Password</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Name</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

**Magento** is a fraud prevention, detection and advisory service. It maintains a globally accessible registry of authentication information so that consumers, financial institutions, retailers, businesses and governments can assess the validity and trustworthiness of the credentials and products they rely upon in the course of online identification, payment, and other important transactions. Additionally, Magento provides token management and cryptographic services, vital to the protection of cardholder data, the payment system, and personal or sensitive information. Magento is a subsidiary of MagTek, Inc.
Enhance your user experience with secure mutual authentication for mobile and online transactions. The secure card reader authenticator is a secure hardware token that performs mutual authentication to the web or mobile apps and host, guarding against automated phishing bots and scripts, transparently and securely logging users into their stored accounts.

**eCommerce authentication stages**

**Stage 1: Hardware authentication**

1. User connects SCRA to Internet device, visits eCommerce site, & activates the Authentication Mode.
2. Website sends Challenge Request to SCRA.
3. SCRA transmits Encrypted Reader Challenge to Magensa.
5. Magensa sends the Encrypted Activation Response to the SCRA.
6. SCRA compares Encrypted Activation Response to expected Encrypted Activation Response.
7. Green blinking LED on SCRA indicates hardware token validation.
8. User manually enters in any form data or payment data and submits to website.
9. Website completes customer service per standard procedures.
10. Internet user receives a response.

**Topology Key**
- Challenge Request
- Encrypted Reader Challenge
- Encrypted Activation Response
- User
- User time
- SCRA hardware token
eCommerce authentication stages

Stage 2: Hardware authentication and username validation

Make login easier and more secure by using secure card reader authenticators and a username. The hardware token replaces the need to remember passwords and delivers mutual device/host authentication and when used with a username also provides multi-factor authentication. Login is easier checkout is faster resulting in lower cart abandonment.

1. User connects SCRA to Internet device, visits eCommerce site, & activates the Authentication Mode

2. Website sends Challenge Request to SCRA

3. SCRA transmits Encrypted Reader Challenge to Magensa

4. Magensa Decrypts SCRA Challenge & formulates Encrypted Activation Response

5. Magensa sends the Encrypted Activation Response to the SCRA

6. SCRA compares Encrypted Activation Response to expected Encrypted Activation Response

7. Green blinking LED on SCRA indicates hardware token validation

8. User enters User Name and submits.

9. Website validates User Name.

10. Website sends validation.

11. User manually enters in any form data or payment data and submits to website.

12. Website completes customer service per standard procedures

13. Internet user receives a response.
Users can enter in their current username and passwords but have the added security of the hardware token to perform mutual device/host authentication. This introduces transparent multi-factor authentication without changing your current login process.

**PC Client**

1. User connects SCRA to Internet device, visits eCommerce site, & activates the Authentication Mode

2. Website sends Challenge Request to SCRA

3. SCRA transmits Encrypted Reader Challenge to Magensa

6. SCRA compares Encrypted Activation Response to expected Encrypted Activation Response

7. Green blinking LED on SCRA indicates hardware token validation

8. User enters User Name, and Password

11. User manually enters in any form data or payment data and submits to website.

13. Internet user receives a response.

**WebSite Server**

2. Website sends Challenge Request to SCRA

4. Magensa Decrypts SCRA Challenge & formulates Encrypted Activation Response

5. Magensa sends the Encrypted Activation Response to the SCRA

6. Secure via 3DES Encryption & DUKPT key management

8. Website validates User Name & Password

10. Website sends validation.

12. Website completes customer service per standard procedures

**Magensa**

3. In the clear, no need to encrypt.

4. Secure via 3DES Encryption & DUKPT key management

6. Secure via 3DES Encryption & DUKPT key management

7. Data: Secure via SSL, Server Certificates, IP Address

9. Website validates User Name & Password

11. Website completes customer service per standard procedures

**Topology Key**

- User
- User Name
- User Time
- SCRA Hardware Token
- User Password
- User Name

© Copyright 2012 Magensa All rights reserved. Page 4 of 5 PN 99810012 rev 2.01 2/12

Magensa I 1710 Apollo Court, Seal Beach, CA 90740 I 562-546-6500 I info@magensa.net
For maximum security, use the hardware token for mutual device/host authentication and use a card swipe for card and user authentication. This takes security to the highest level, providing “card present” authentication. The username can be extracted directly from the authenticated card for unparalleled transaction authentication, while at the same time transparently and securely logging users into their stored accounts.