












ECOMMERCE STAGES OF AUTHENTICATION

DYNAMIC FACTOR AUTHENTICATION



Topology Key

-  Challenge Request
-  Encrypted Reader Challenge
-  Encrypted Activation Response
-  Card Data, User name & Password
-  MagnePrint Score
-  User
-  User time
-  SCRA hardware token
-  User card swipe
-  User Password
-  User Name

	Stage 1	Stage 2	Stage 3	Stage 4
Hardware authentication	X	X	X	X
Mutual device authentication	X	X	X	X
Single factor authentication	X	X	X	X
Faster login	X	X	X	X
Web app validation	X	X	X	X
Guards against phishing	X	X	X	X
Guards against bots/scripts	X	X	X	X
Multi-factor authentication		X	X	X
Unique user validation		X	X	X
User authentication				X
Card authentication				X
Enhanced user experience				X
Faster checkout				X
Card present purchase				X
Guards against keystroke logging				X
Ability to share SCRA's				X

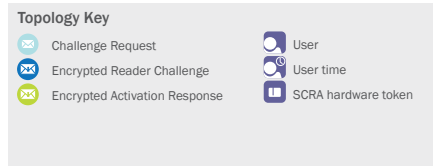
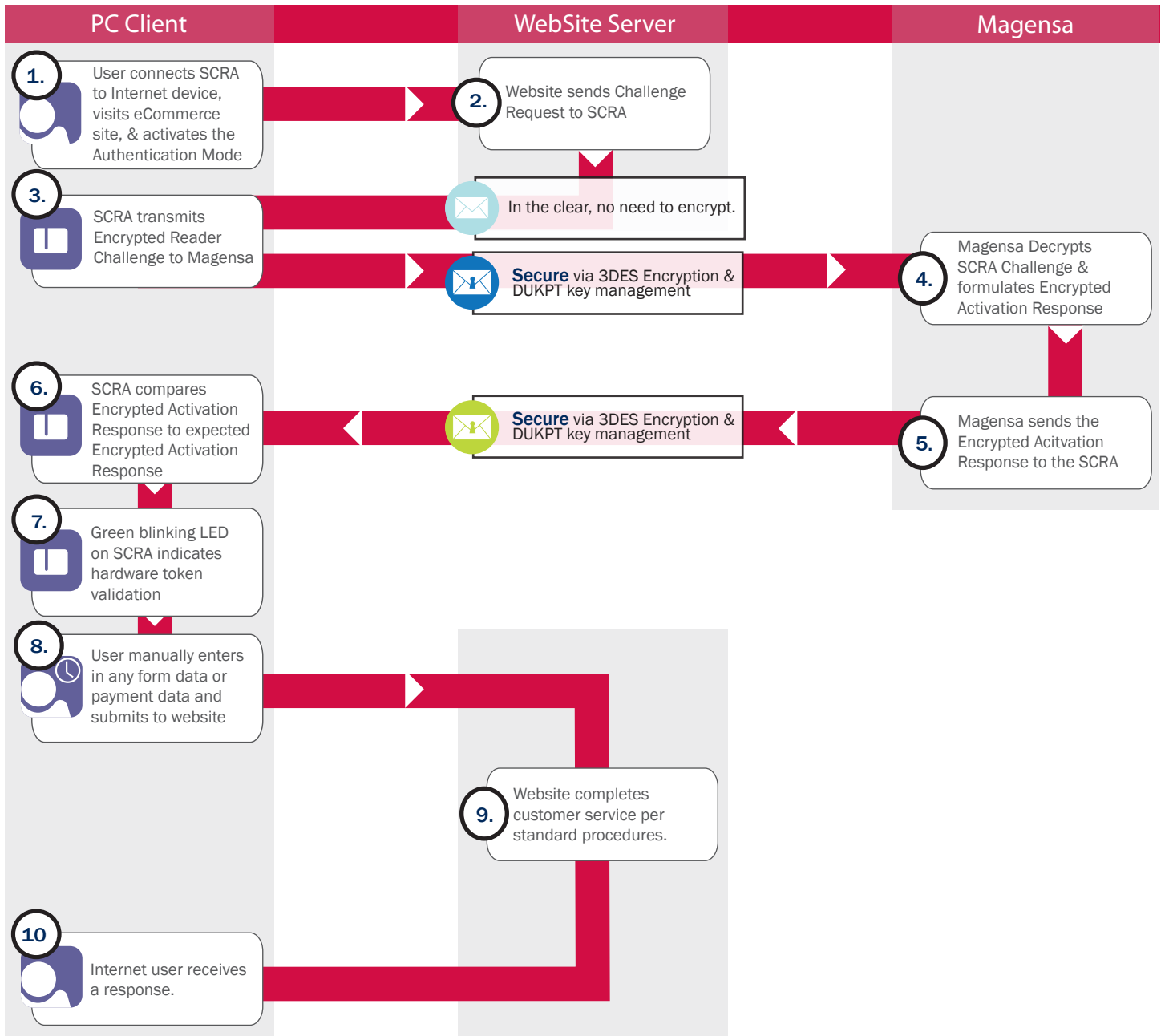
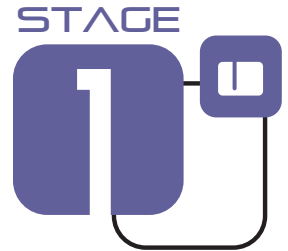
Magensa™ is a fraud prevention, detection and advisory service. It maintains a globally accessible registry of authentication information so that consumers, financial institutions, retailers, businesses and governments can assess the validity and trustworthiness of the credentials and products they rely upon in the course of online identification, payment, and other important transactions. Additionally, Magensa provides token management and cryptographic services, vital to the protection of cardholder data, the payment system, and personal or sensitive information. Magensa is a subsidiary of MagTek, Inc.



eCommerce authentication stages

Stage 1: Hardware authentication

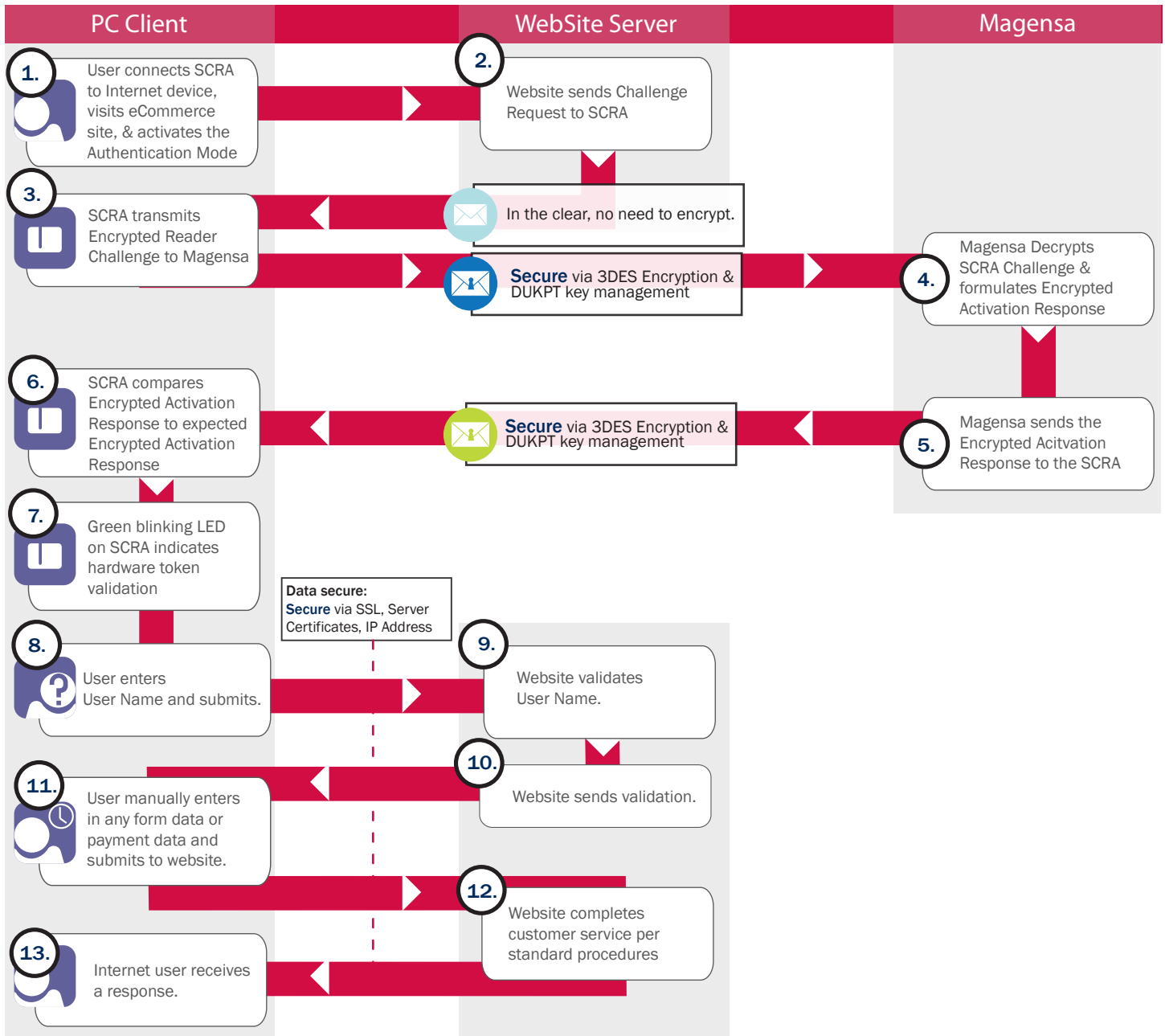
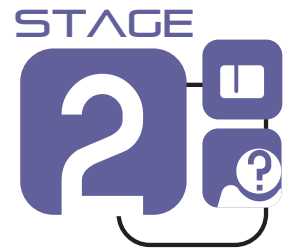
Enhance your user experience with secure mutual authentication for mobile and online transactions. The secure card reader authenticator is a secure hardware token that performs mutual authentication to the web or mobile apps and host, guarding against automated phishing bots and scripts, transparently and securely logging users into their stored accounts.



eCommerce authentication stages

Stage 2: Hardware authentication and username validation

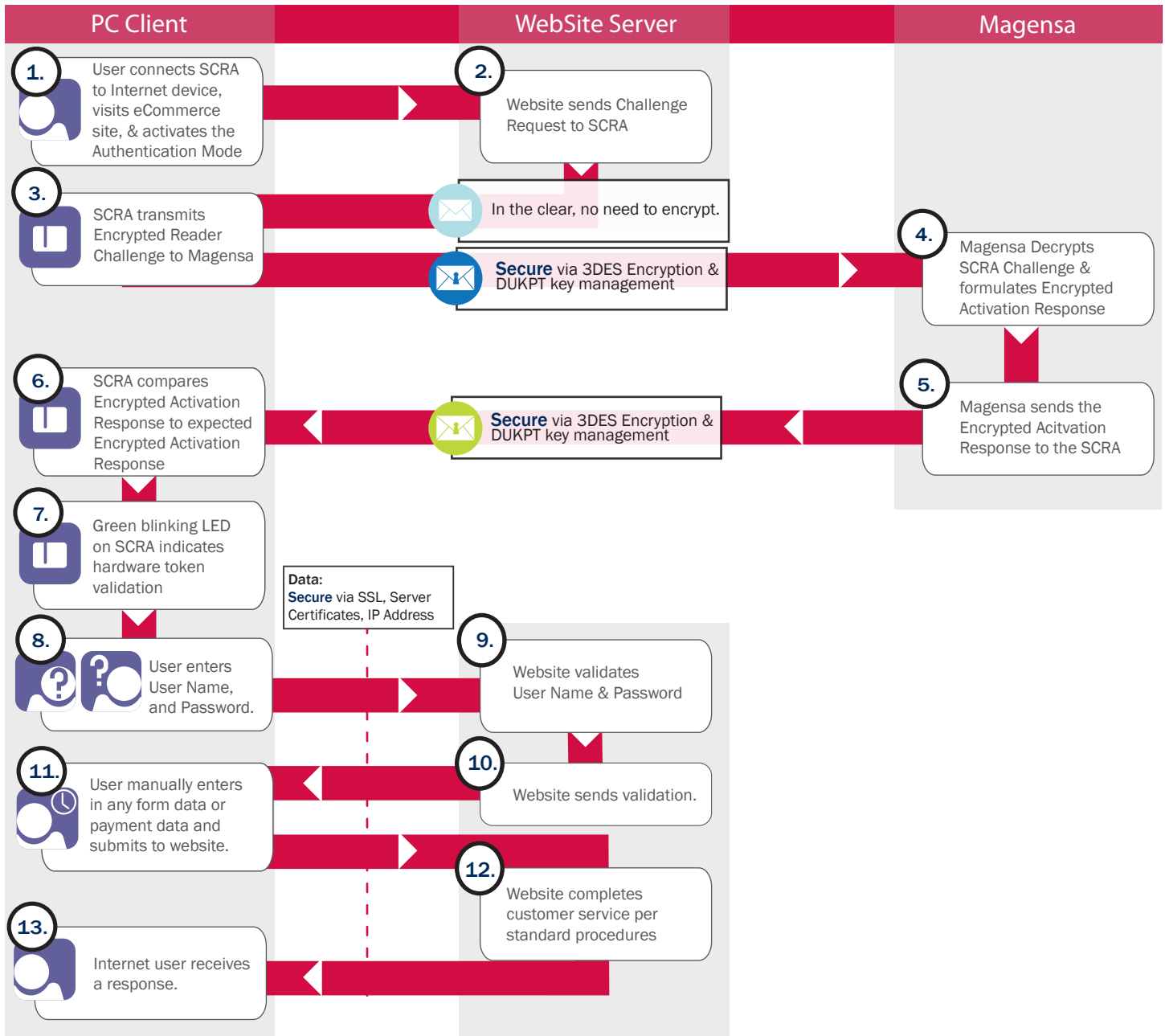
Make login easier and more secure by using secure card reader authenticators and a username. The hardware token replaces the need to remember passwords and delivers mutual device/host authentication and when used with a username also provides multi-factor authentication. Login is easier checkout is faster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



eCommerce authentication stages

Stage 3: Hardware authentication and username and password validation

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.



eCommerce authentication stages

Stage 4: Hardware, User, Card, cardholder authentication



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.

