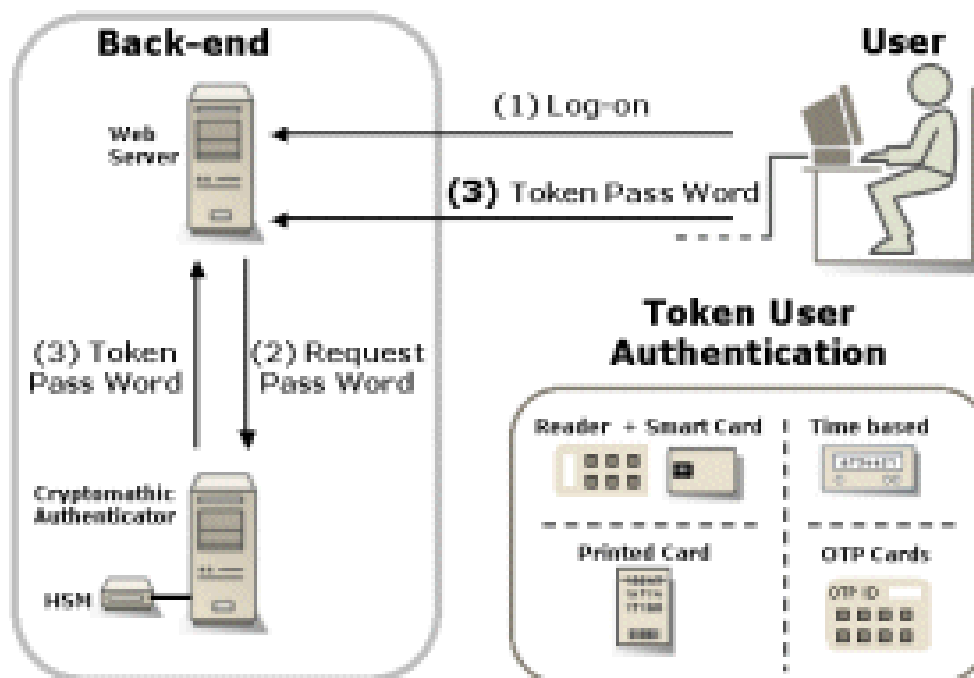




Cryptomathic Authenticator

Cryptomathic Authenticator is a secure web authentication solution. Alongside traditional static username and passwords it provides strong two-factor authentication via independent channels. Options for authentication methods are endless and include SMS, one-time passwords (OTP), secure tokens, mobile readers and cards, scrape off tokens etc. Cryptomathic Authenticator is easily integrated with existing back-end systems and infrastructure.

Token User Authentication



Cryptomathic Signer is a signature server: it stores the user's private signature key securely in a central database and generates digital signatures on the user's request. The user can request a signature at any time, e.g. from a Web browser or an e-mail client.

With Signer the physical security of the private key is no longer the user's responsibility, as it is not stored on a personal computer or hardware token. However, strong authentication ensures that the private key remains under the user's sole control, and she can use it from any connected device.

An Improved Solution

Compared to traditional key storage solutions, i.e. software and smart cards, Cryptomathic Signer offers:

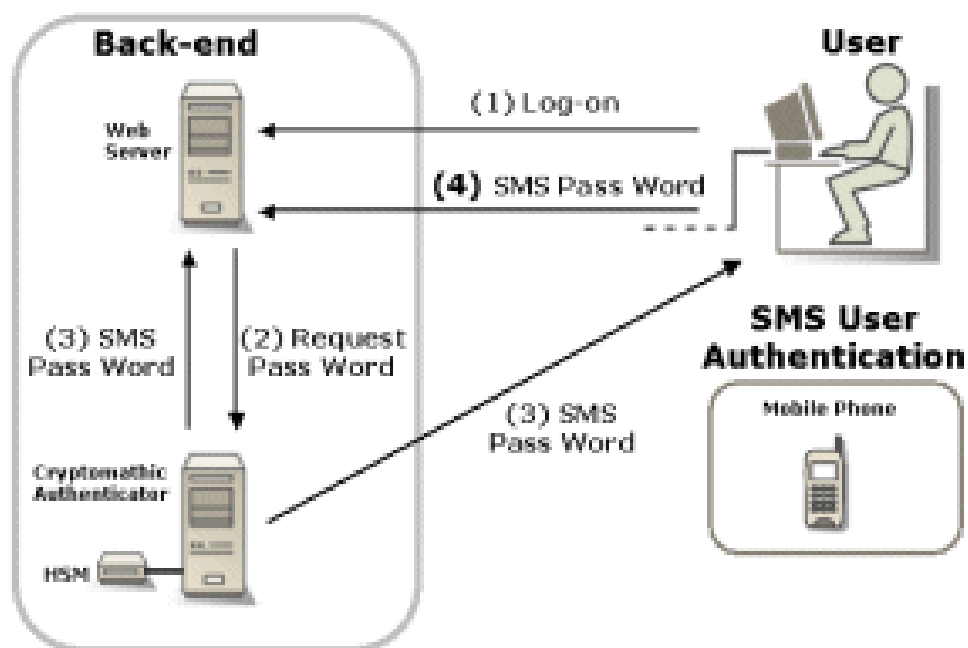
- **Enhanced Key Protection** – The private key is generated in and never leaves the server's high security environment
- **Enhanced Security** – The private key is protected by the user's password at all times, and not even the Signer service provider can access the key
- **Mobility** – Signer can always be reached and does not require installation of software at the client side
- **Central Key Management** – Simplifies otherwise complex tasks like key renewal and policy enforcement

Cryptomathic Signer is designed for Common Criteria EAL 4+ compliance

Anti-phishing

Web transactions need to be secured against fraud and loss of consumers confidence. The Cryptomathic Authenticator fights phishing, man-in-the-middle and other security-related attacks offering businesses the solution needed to fight fraud and retain on-line customers.

SMS User Authentication



Multiple authentication methods

Almost any type of token is supported by the Cryptomathic Authenticator, including grid cards, time-based tokens, OTP cards, OTP SMS, key-ring tokens, disconnected smart card readers, connected readers, finger-print biometry, etc. Various protocols are supported for addressing customer-

specific needs, e.g. challenge-response and RADIUS. Depending on requirements the system provides user and / or message authentication, thereby providing the highest possible level of security.

Channel independence

Because our customers have a large diverse client base they require user-friendly solutions. The Cryptomathic Authenticator has in-built flexibility in choice of the user channels, - e.g. web, GSM, fixed line phone, fax, mail - to satisfy almost any end-user need.

Integration

The Cryptomathic Authenticator is designed to integrate seamlessly with existing solutions to minimise the impact on legacy systems. It can integrate with an existing customer / user database and plugs into existing authentication methods, e.g. an SMS gateway. It also support various applications - e.g. web banking and corporate payment systems - and Cryptomathic can integrate with provisioning systems such as token ordering and distribution.

Future proof

The Cryptomathic Authenticator is a solid investment as it meets current and future requirements, e.g. new technology supported by Cryptomathic like CAP or digital signatures

Contact eB2Bcom

Sydney: +61 - 2 - 9779 -1597
Melbourne: +61 - 3 - 9896 -7800
email: sales@eb2bcom.com
Web: www.eb2bcom.com