H-Login

Overview

The first step common to all modules of the H-Apps suite is the user authentication procedure required to gain access to any application resources and to the isolated execution environment. These tasks are handled by the H-Login module which allows users to setup their secret credentials (username and passphrase, or PIN and PUK when the module is interfacing with a Smart Card) and which can set up a hardened desktop environment inside of which the H-Apps will be running.

The H-Login module allows also entering the general settings for network connections (e.g. proxy authentication credentials), as well as user preferences (default language, auto-logoff time, H-Apps startup priority, etc.). Furthermore, the H-Login handles communication with the H-Server enabling the Proactive Security Updates of the licensed H-Apps and the remote management of the user access to any deployed hardware devices (e.g. smart USB drives).

Main Features

- Zero-footprint (no prior installation, special drivers or admin privileges required to run on the host PC)
- Enforces corporate policies for end user enrolment and authentication. Can interface with any authentication server and transaction protocol.
- Supports mutually authenticated network access to safeguard from man-in-the-middle and host tampering attacks
- Enforces integrity checks on all application components and updates before allowing execution
- User interface localized in English, French, German, Italian. Additional languages available upon request.
- (Optional) Establishes the H-Desktop, a hardened, lightweight virtual operating environment isolated from host applications, capable of operating securely also in the presence of active malware
- (Optional) Provides active protections against the following attack vectors:
  - Screen Capture
  - Windows Overlay
  - GUI Controls Manipulation
  - Keystroke Logging
  - Mouse Logging
  - Keystroke Event Emulation
  - Mouse Event Emulation
  - Function and code injection
- Enables the centralized cloud-based management of the H-Apps, allowing to receive Proactive Security Updates from the H-Server and to block access to the H-Apps resources and data.

For more information, please visit: http://www.eisst.com

System Requirements

Processor	IBM PC or compatible with Intel base processors Intel Pentium 4 800-MHz or higher (Intel Core 2 Duo or higher recommended)
Memory	512 megabytes (MB) of RAM (2GB recommended)
Operating System	Microsoft® Windows® XP SP3 or higher Microsoft® Windows® VISTA all versions Microsoft® Windows® 7 all versions Microsoft® Windows® 8 all versions Microsoft® Windows® 8.1 all versions Mac OSX 10.6.x and higher
Display	1024 x 768 resolution, 65 536 colors minimum (32-bit color recommended)

Sample Images

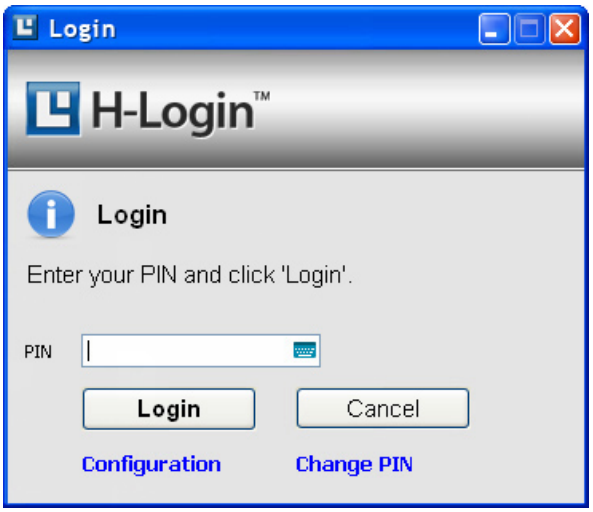

Fig. 1 The main application window of H-Login allows entering the authentication credentials required to access the application/device resources and to setup the isolated execution environment (H-Desktop) inside of which the H-Apps will be running. Clicking on the keyboard icon at the right of the PIN entry field opens the Virtual Keyboard window (ref. Fig. 2).

Fig. 2 The Virtual Keyboard (VK) and Mouse Pad allow protecting against both keystroke and mouse logging. The users can either click directly with the PC mouse pointer on the VK's buttons or operate the virtual mouse pointer before selecting which button to click.

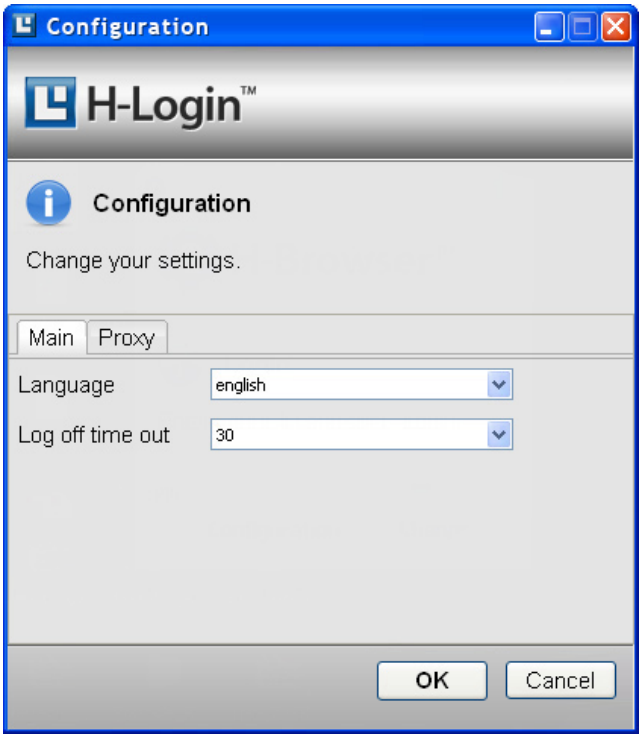

Fig. 3 The H-Login module allows indicating the default settings (language, auto-logoff time, H-Apps startup priority, *etc.*), setting the proxy options for network connection, and accessing security features and product versioning information.

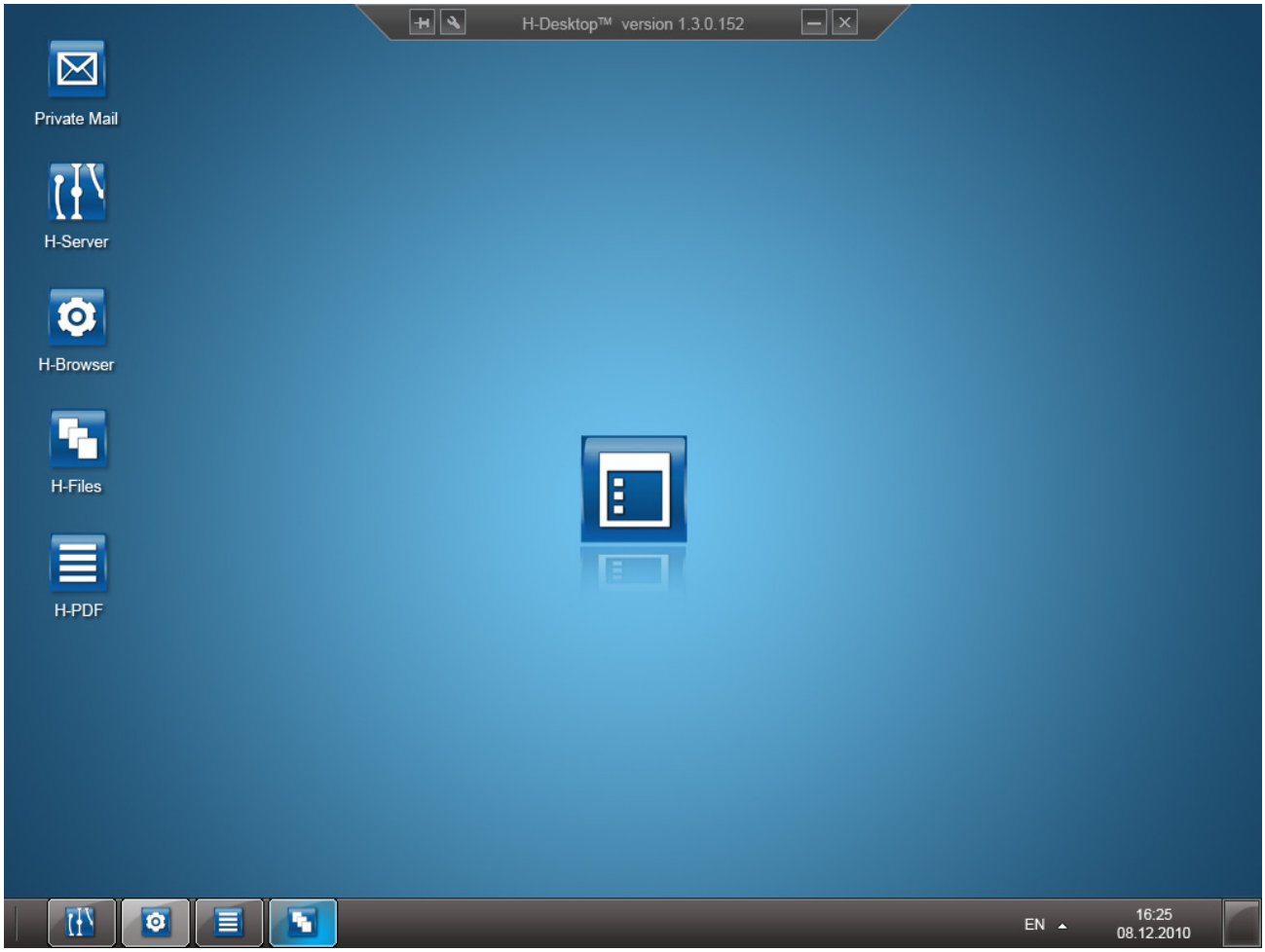

Fig. 4 The H-Desktop is an optional component of the H-Login application which enables running the H-Apps inside of an isolated and protected execution environment. Users can switch from the H-Desktop to the host PC desktop (and vice versa) with a single mouse click. The H-Desktop enables protections against attack vectors targeting the user interface (*e.g.* screen capture) and the application's execution environment (*e.g.* code injection).