



vLAD-1 Vlatacom Login & Access Device

Product Description

vLAD-1 is a device for biometric access control to logic resources. The device is used in systems that require a high level of security in the authentication process. The user is authenticated by matching the following three components: 1) something the user has (i.e. the smart card), 2) something the user knows (i.e. the PIN), and 3) something the user is (i.e. the fingerprint). A smart card containing Match-on-Card technology performs the template and live fingerprint matching, which means that the template fingerprint is never exposed outside the card and the live fingerprint is never exposed outside the vLAD device. In addition to user authentication, mutual authentication between the vLAD device and the workstation is also performed, which prevents potential abuse involving the replacement of devices or workstations. The device is authenticated by using a digital certificate stored in the security access module (SAM).

Key features

- Three-factor authentication:
 - a) Smart card - contact, ISO/IEC 7816, ID-1
 - b) Fingerprint
 - c) PIN
- Smart card supporting Match-on-Card technology
- Built-in security access module with contact smart card (ISO/IEC 7816, ID-000)
- vLAD messages are digitally signed with private keys from the SAM module and the user's smart card
- Optional encrypted communication between the vLAD device and the workstation
- USB interface to workstation
- LED user interface
- Power supply: USB
- Size: 87 x 71 x 27 mm
- Supported OS: Windows 32-bit and 64-bit, Linux and MacOS





Market

vLAD-1 is suitable for use in all systems that require strong authentication of users with maximal protection of the user's personal data. Such systems comprise the large public entities - law enforcement, military, postal services, but also enterprise companies, banks, and similar. Practically, vLAD-1 can fit all systems that use the public key infrastructure (PKI).

vLAD-1 may also find its use in on-line services that require powerful and reliable user authentication such as e-banking, internet payments, etc.

Use Cases

Access control of employees and officers to logical resources - many public institutions, law enforcement, banks, et al require strict control of access to information and programs. Due to its reliable authentication on one hand, and protection of private information on the other, vLAD-1 is the ideal solution for access control to logical resources in such systems.

Internet services end-users authorisation - Internet payments and other banking transactions may expose the users to the risk of fraudulent use of their sensitive personal or banking data. By using the vLAD-1 device and the appropriate infrastructure, such risks are significantly reduced.

The use of vLAD-1 device prevents:

- Unauthorised use of IT systems
- Fraud in IT systems

Using vLAD-1 for the authorisation of financial transactions prevents the theft of sensitive data. vLAD accomplishes this goal by removing sensitive data from the reach of Internet service operators. The card holder's authentication is carried out within the device itself, and the only data sent to the Internet service operator is the digitally signed authentication result.

Key Benefits

- Three-factor user authentication
- Match-on-Card technology
- Maximal protection of biometric data
- Mutual authentication of the vLAD device and the workstation
- Digitally signed messages and optional encryption
- Protected against abuse attempts such as replacing the device or tapping into the communication between the device and the workstation



Address:
Vlatacom institute d.o.o.
Milutina Milankovića 5
11070 Belgrade, Serbia

tel: +381 11 377 11 00
fax: +381 11 377 11 99
info@vlatacom.com
www.vlatacom.com