

REMOTE WORKER – ACCESS SOLUTIONS



There are many potential use cases for CardLab's Access and Defender families of access cards with embedded fingerprint sensors in the context of remote worker access:

Physical access control: Biometric cards can be used to grant remote workers access to physical facilities or areas that require secure access, such as offices, data centers, or laboratories.

Network access control: Biometric cards can be used to grant remote workers access to network resources, such as servers, applications, or data storage.

Remote desktop access: Biometric cards can be used to grant remote workers access to their desktop environment when working remotely, allowing them to access the same resources and applications as if they were in the office.

Single sign-on (SSO): Biometric cards can be used to enable single sign-on (SSO) for remote workers, allowing them to access multiple systems and applications with a single set of credentials.

Time and attendance tracking: Biometric cards can be used to track the attendance and work hours of remote workers, helping organizations to accurately record and monitor employee time.

Regulatory compliance: Using biometric cards can help organizations meet regulatory requirements for secure access and data protection



Access and Defender cards – at a glance:



- Match on card fingerprint sensor for verification
- No requirement to upgrade installed readers
- Supports multiple reader types via RFID
- Optional display for information data
- Embedded record storage option
- GDPR compliance through identity tokenization
- User artwork according to card industry standards
- Multiple personalization options

Solution benefits: The Access and Defender cards have been designed to work with multiple readers and can work with existing infrastructure. Biometric data is stored only on the card so there is no requirement to manage databases of biometric data with its inherent hacking risk. With an RFID or optional contact or Bluetooth interfaces, the card can serve as the authentication devices for any host platform including tablets, PC's, door locks and other terminals, and will function without any special upgrades to the backend as all is based on authentication API's. Only by presenting the correct, registered finger, can the card and any stored data be activated and prove your identity.



Are you ready to secure your organization?

Learn how CardLab's Access, Defender,
and Quardlock Backend solutions
can protect your enterprise while
simplifying user experience.



CARDLAB APS

HOERKAER 20, 2
DK-2730 HERLEV
DENMARK

EMAIL: INFO@CARDLAB.COM

PHONE: +45 31 55 49 94

CARDLAB (THAILAND) CO. LTD.

200/9 MOO 2 KLONG TAMRU
MUANG CHONBURI 20000
THAILAND

EMAIL: INFO.ASIA@CARDLAB.COM

PHONE: +66 38 195 193

