Tri-factor Authentication for Access Control at DRDO (Defense Research and Development Organization)

Vertical: Defense

Date: October 2017

"IDCUBE provided customized multi layer authentication system at DRDO, consisting of two modules, a mobile enrollment unit and an authentication station"

REQUIREMENTS:

- Multi level authentication
- Alarm generation

Defense Research and Development Organization (DRDO) works under the Department of Defense Research and Development of Ministry of Defense, Government of India. DRDO work in various areas of military technology which include aeronautics, armaments, combat vehicles, electronics, instrumentation engineering systems, missiles, materials, naval systems, advanced computing, simulation and life sciences.

PROBLEM STATEMENT

As a functioning body of the Indian defense system, DRDO required a highly secured authentication system for providing physical access into critical zones such as laboratories and control rooms. The system was also required to identify any unauthorized attempt to enter a secured zone and notify the authorities.

SOLUTION

IDCUBE provided customized multi layer authentication system for DRDO's highly secured zones. The system consists of two modules, a mobile enrollment unit and an authentication station. The user enrollment is done using the mobile enrollment unit. During the enrollment process, the unit is taken to senior officials for obtaining their biometric credentials.

After the completion of enrollment process, data from the unit is synchronized with the primary server and the authentication station. The authentication station is equipped with three types of identification devices, that is, an IRIS scanner, a multispectral fingerprint reader and a Scramble PIN pad. Any two of the credentials should be provided by a

APPLICATION/ PRODUCTS:

- Biometric Devices (IRIS+ Finger Print+ PIN)
- Customized vault
- Fiber optic networking equipment
- Customized rugged briefcase

user in order to enter a protected zone. The system logs including an unauthorized attempt are transferred to the primary server in the real time.

RESULT

- IDCUBE provided tri-factor authentication system at DRDO for the highly secured zones.
- The authentication unit is further protected from physical access using a PIN pad reader, to be operated by security personnel.
- Access denied alarm is raised in the control room in case an unauthorized user attempts to enter. The primary server further integrates with CCTV cameras to monitor the authentication unit.
- The system records all access and alarm logs.

SYSTEM ARCHITECTURE