

## Dozens of data centres equipped

Whether because of the sensitivity of the data they contain or the criticality of their business continuity, data centres must implement enhanced security measures.

Faced with the risks of hacking, espionage or sabotage, impermeability must be ensured by strong authentication solutions (biometrics, dual identification, video control, etc.) and security (encryption, security keys, etc.).

Through its solutions and its ANSSI qualification, TIL TECHNOLOGIES can meet all the needs of this type of sensitive sites.

### TIL ALREADY EQUIPS

#### DATA CENTRES EN FRANCE

- DCFORDATA - Limonest
- EQUINIX DATA CENTRE - Pantin
- TDF DATA CENTRE BOULIAC - Bouliac
- ANTONY TERADATA - Antony
- ANGERS TERRENA - Angers
- IBO DATA CENTRE - Clermont-Ferrand
- DS SMITH DATA CENTRE - Kayserberg
- DATA CENTRE CEGEDIM LABEGE - Labège
- MARAIS DATA CENTRE - Paris
- MARSEILLE LOCAL DATA CENTRE - Marseille
- CREDIT AGRICOLE HEADQUARTER DATA CENTRE - Paris

#### DATA CENTRES À L'INTERNATIONAL

- DATA CENTRE ADMINISTRATION DEFENSE NATION - Rabat (Morocco)
- DATA CENTRE BMCE - Casablanca (Morocco)
- DATA CENTRE UNIVERSITE D'ABIDJAN - Abidjan (Ivory Coast)

## DATA CENTRES



ADAPTED SOLUTIONS  
TO EVERY SECTOR



**TIL TECHNOLOGIES**  
ELECTRONIC SECURITY SYSTEMS



OPTIMISE OPERATIONS

- **Single graphical interface** for access control, intrusion, video, interphony and technical alarms
- **Archiving and research of related events** (alarms, passage of employees, videos...)
- **Software gateways** to applications or third party databases to prevent errors or double entry
- **Assistance to the Internal Operation Plan** with real time registration in secured/unsecured areas

PROTECT THE SYSTEM, DATA AND COMMUNICATIONS

- **Prevent badge piracy:**
  - Secured badges, diversified encryption key for each user
- **Anti-piracy of system and communication:**
  - Transparent readers and full hardware architecture ANSSI qualified
- **Continuity of operation:**
  - Offline mode of the readers and control unit in case of network failure
  - Server redundancy, real or virtualised
- **History of operator actions** to control the security agents

FILTER AND IMPROVE FLOWS

- **Vehicle access management:**
  - Car plate recognition
  - Long distance badges
- **Office filter:**
  - Autonom mecatronic readers, online or offline (rights in the badge)
- **Lift management:**
  - Access to authorised floors

MANAGING VISITORS AND SUBCONTRACTORS

- **Visiting process:**
  - Pre-registration of appointments
  - Validation from the superior
  - Physical reception or on a touch display
  - Scan of the identity document
  - Badge loan, instructions, escort
  - Real-time presence monitoring

MONITOR THE SITE AND ITS SURROUNDINGS

- **Perimeter intrusion detections:**
  - Active gates, infrared barriers
- **Video surveillance**
  - Real time observation or event doubt removal
- **Field inspections:**
  - Control of badges and authorisations by mobile reader
  - Round assistance tool and on-site patrolling assistance

REINFORCED ACCESS CONTROL

- **Strong authentication for the sensitive zone:**
  - Access through biometric reader or strengthened control badge + code
  - Use of unicity equipment, mantrap and turnstiles
  - Remote opening with video control
- **Fine rights management:**
  - Assignment of rights according to profiles, grades, technical authorisations, time slot and validity date
- **Control of the on-site moves:**
  - Manangement of the closed areas, anti-passback system and real-time census

