CASD

CENTRE D'ACCÈS SÉCURISÉ AUX DONNÉES

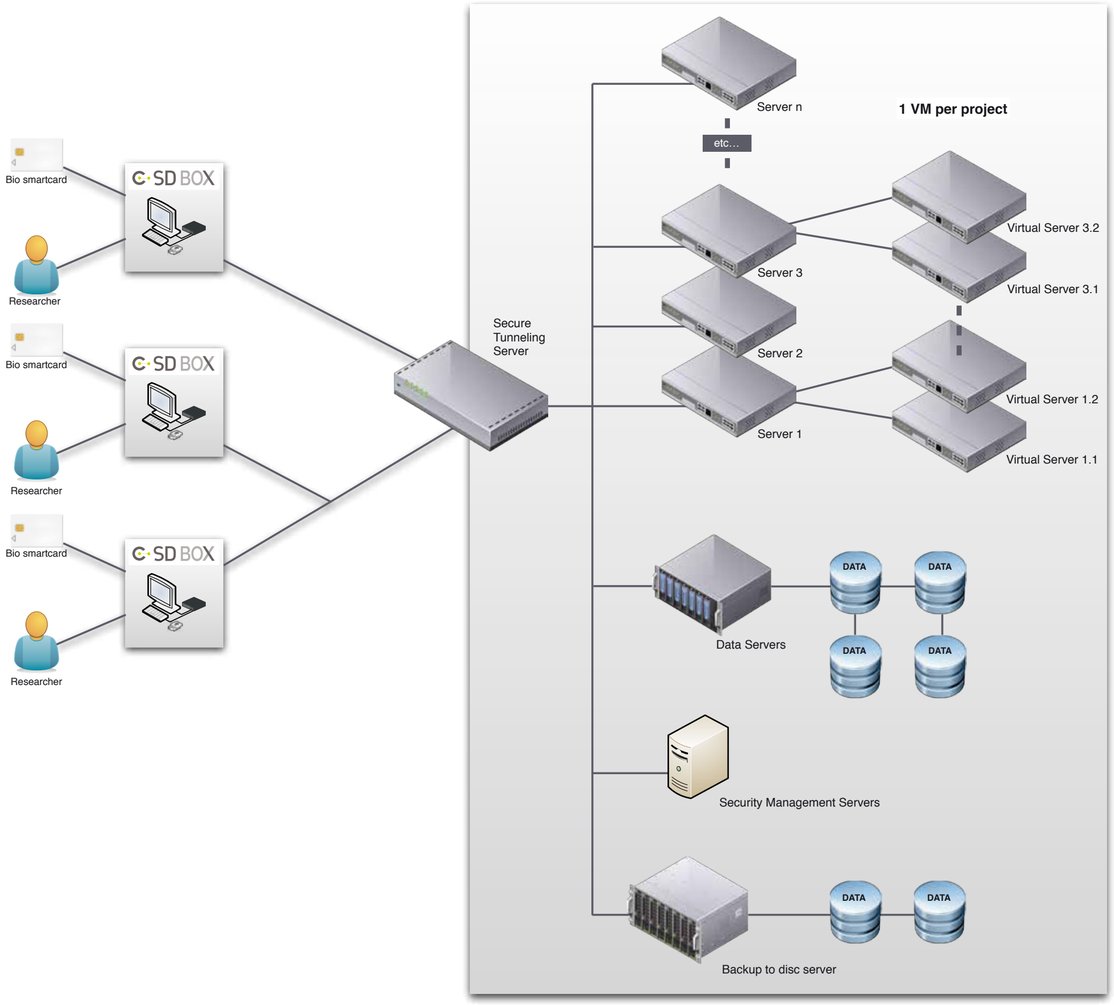
Description of the CASD Remote Access architecture

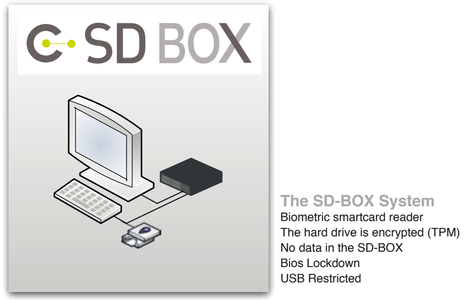
The architecture of the CASD (Remote access) has been designed by the GENES IT Department to take into account many constraints such as:

- High security constraints: including a biometric strong authentication and no data leak;

- Ergonomic constraints: researchers need for computer interfaces and tools that enable them to work in excellent conditions;

- Integration constraints: the CASD architecture must be easily integrated into the pre-existing computer environment at the researchers' institutions.





The SD-BOX System
Biometric smartcard reader
The hard drive is encrypted (TPM)
No data in the SD-BOX
Bios Lockdown
USB Restricted

To deal with these constraints, the concept introduced by the GENES relies on a distributed architecture based on:

- An innovative secure device installed in the researcher's laboratory: the SD-Box;

- A remote secure servers farm hosting confidential microdata and a set of scientific software;

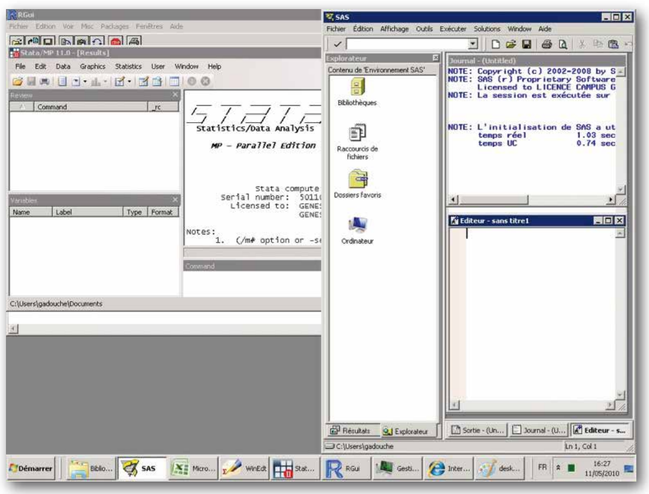
From the researcher's perspective, everything is at hand: data, software, storage, computing power… as if it was a powerful machine on his desktop; but in fact everything is happening on the secure servers inside the CASD center; everything is remote except the screen and keyboard/mouse.

CASD

CENTRE D'ACCÈS SÉCURISÉ AUX DONNÉES

Main features : Security

The SD-Box is an interface between the researcher and his project server. It is a secure device (hardened device), tampering proof, impervious to eavesdropping and network attacks. It is remotely authenticated, monitored and configured from the CASD centre of operations. Communications between the SD-Box and the CASD centre are encrypted.
- To access his project, a researcher must authenticate with a biometric smartcard.
- The whole CASD system is a closed environment: through encrypted tunnels between the SD-Boxes and the servers
- The researchers only have their keyboard to introduce data by themselves, and they have no opportunity to download, print out nor copy and paste any data. Every input / output is controlled by authorised staff.
- SD-Box are not dependent from an unknown and uncontrolled system that may be insecure. (system vulnerable, not updated, compromised…).
- Centralized security management (patches distribution…).
- Firewall protection : the SD-Box communicates only though a secure channel. SD-Box can be disabled remotely.
- SD-Box are authenticated.



- **Deployment:**
  The CASD system does not require specific deployment process and does not rely on local IT infrastructure.
  The SD-Box only requires a small set of services from the local network environment. It just needs to communicate with the CASD centre of operations through Internet. There is no complex setup procedure; no integration tests to run, no compatibility issues. All this operations are expensive in time and in money.
- **Servicing / supervision:**
  SD-Boxes are managed from the CASD centre of operations. They can be monitored, configured and upgraded remotely. This enhances the security level.
- **Assistance:**
  SD-Boxes are identical. In case of failure, replacement is straightforward.
- **User Experience :**
  The virtual server provides the researcher a well-known environment (desktop) with everything he needs to work: datasets, processing power, memory, storage and scientific software.
- **Cost:**
  The cost of the CASD equipment for researchers is far lower than the cost for current software solutions, which includes more expensive licence fees, installation, servicing and helpdesk costs.
  The SD-Box can be shared by several projects (at least 2). There is no complex setup procedure; no integration tests to run, no compatibility issues.