The Configuration System is the “glue” that ties all DIRAC systems together. Any piece of DIRAC needs the CS to know where are the other parts of DIRAC. Because of that, it was designed with stability as primary goal. To reach a 24/7 uptime, CS servers can be added easily to the system to increase redundancy and reduce the load on existing ones.

The CS has a master server that has a complete copy of the DIRAC configuration. This server is the only one that allows administrators to change the configuration. To propagate the configuration, slave CS servers contact the master server periodically asking for changes. If the master server holds a newer version of the configuration the slave server downloads it.

CS clients have a configuration cache. So when a client asks for some configuration, it is responded from the cache instead of having to connect to CS servers. This configuration cache also queries periodically to any configuration server for newer versions of the configuration.

All DIRAC components rely on a low level framework that provides the necessary basic functionality. This framework contains:

- DISET: DIRAC’s secure communication protocol for RPC and file transfer.
- Configuration System: Providing redundant distributed mechanism for configuration and service discovery.
- Logging and Monitoring System: Uniform way for all components to report their status and activities.
- Web site: Interaction interface to systems and visual representation of their status and activities.

DISET (DIRAC SEcure Transport) is the DIRAC secure transport layer. It takes care of all the communication between DIRAC components. DISET provides:

- Network connectivity using standard TCP/IP;
- When a secure connection is requested, DISET uses OpenSSL through a modified python binding. This provides grid authentication and encryption, using X509 certificates and grid proxies;
- Object serialization for standard python types.
- Per method user and group authorization. Authorization rules can be defined and automatically propagated through the Configuration System.

DISET provides RPC and file transfer capabilities to DIRAC Services, allowing multiple threads. Only the server’s functionality has to be coded.

When exposing RPC capabilities, DISET automatically checks the types of the call arguments and their status and activities.

The monitoring and logging systems are the representations of the status of the DIRAC setup. DIRAC Services and Agents send their activity reports to the Monitoring, and important messages to the Logging system respectively. Monitoring and Logging Agents process the received data as well as generate reports and statistics for DIRAC users. These reports and statistics are made available dynamically through the DIRAC web site. In case the servers are offline DIRAC Services and Agents will send the data to the Request Service which will forward the data to the final destination once the services are back online.

The DIRAC web site provides a uniform way to present:

- System status for administrators;
- Job information for users;
- General DIRAC information for all.

The web site takes advantage of the Framework to communicate with DIRAC servers and retrieve user’s requested information dynamically. All members of the VO identify themselves by loading their valid certificate into their browsers. Authorized users can then interact with DIRAC Systems via the web site. Administrators are also able to manage DIRAC remotely.