

# Cerberero

## Triple technology Reader

Convergence between Physical and Logical Security  
at Critical Installations



**Digital Signature**



**Fingerprint**



**Alphanumeric Code**

The market conditions and the global environment require those responsible for security to operate intelligent platforms at which the risks inherent in critical processes can be managed effectively and efficiently.

In the traditional security model the security concept is based on a scenario where it is wished to provide the protection of people, values and the infrastructure. This perception of the new integral model encompasses, in addition to the above, the protection of information or knowledge and the processes, products and services inherent in the company and the scope of protection migrates to a global scope from the location mentioned previously.



However, it is vital, in descriptive terms, to understand what the physical security and logical security concepts involve. The objective of **physical security** solutions is to maintain personal, assets, communities and organizations security. By contrast, **logical security** refers to security in the use of software and systems, the protection of data, processes and programmes as well as that of the orderly, authorised access of users to the information which we can find in any security designs of, for example, a CPD. Logical security involves all those measures established to minimise the security risks associated with their daily operations undertaken, deploying information technology.

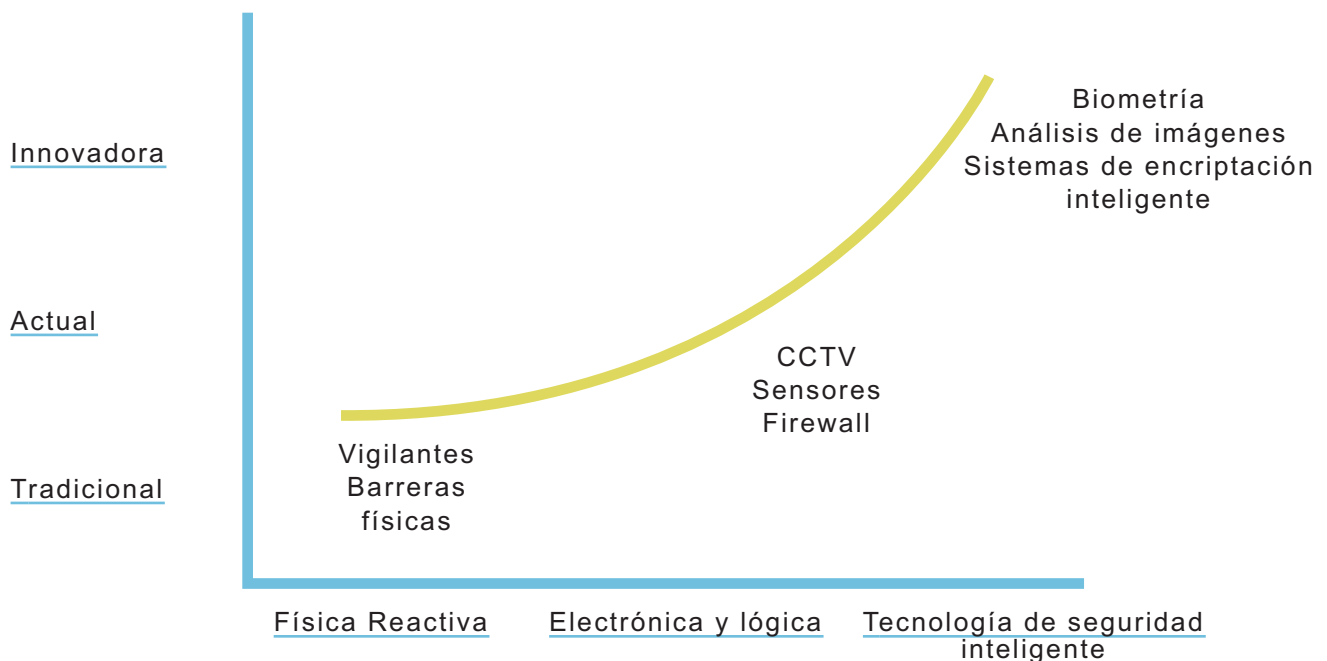
### Evolution

The evolution of security systems goes hand in hand with the evolution of the criminal methods used. In the 1970's the main risks at the time were thefts and robberies and security policy was a reactive physical security policy mainly by means of surveillance (usually human) and physical barriers.

Since the 1990's there was the first major evolution including a significant level of defrauding, falsifications, fraud and asset laundering in criminal impact indices,. It is

at this stage that the concepts of electronic security are consolidated and established as part of the means of physical security established up until then and the logical security concept. As from this stage the main means of protection used are video surveillance systems and sensors in the fields of electronic security and firewalls in logical security areas.

However, on a market which is globalised at all levels a new evolution stage is required. The latest security trends endow physical security systems which predictive, **cryptographic** or analytical methods based on information acquired by means of biometric measurements or image analysis and **digital certificates**.



### Convergence: new security trend.

Until now the worlds of electronic security and logical security have worked concurrently, crossing and even clashing in some aspects of their installation or design concepts.

When ACAL BFI IBERIA started the development of the Cerbero triple technology reader to manage the physical and logical security of a site in a single electronic device (for example, a CPD), the main challenge laid down was the design of a wholly reliable access control terminal. On the one hand, it had to implement the most advanced identification technologies of both sectors (biometrics, cryptography, alphanumeric password and digital signature) and the whole user Registration/Deregistration process from a single hierarchical structure by means of coordination with the "Active Directory" service.

After the initial study of requirements, the document including the technical definition of the services to be implemented was established, based on which the first prototype was carried out. From then until now the Cerbero triple technology reader has grown with the objective of reducing and optimising its operation in user identification and

verification. The current Cerbero state of the art finds itself at its third generation and its flexibility is such that it is able to adapt to diverse, varied operating requirements and even interact in the verification with other systems (locally/remotely) to significantly increase the security level at critical installations such as CPDs.

**Cerbero** it is an access control system geared towards merging and taking advantage of the synergies of implementations at corporate level of both security criteria.

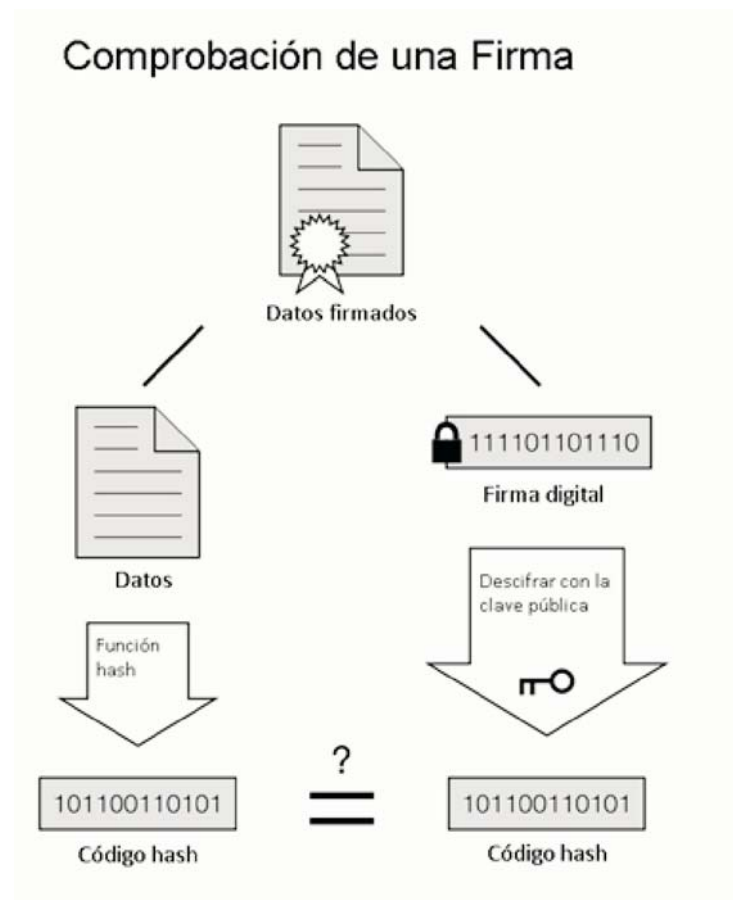
**Cerbero** it is a triple technology access terminal which allows the verification of access to a restricted area to be carried out;

1 By way of biometric fingerprint identification;

2 Access to the card containing the certificates by way of a password.

3 After access to the public content of the card, the digital signature is checked. Cerbero carries out various validations, including the following:

- Validity of the digital certificate of the signatory.
- Revocation of the digital certificate of the signatory.
- Inclusion of time stamp.



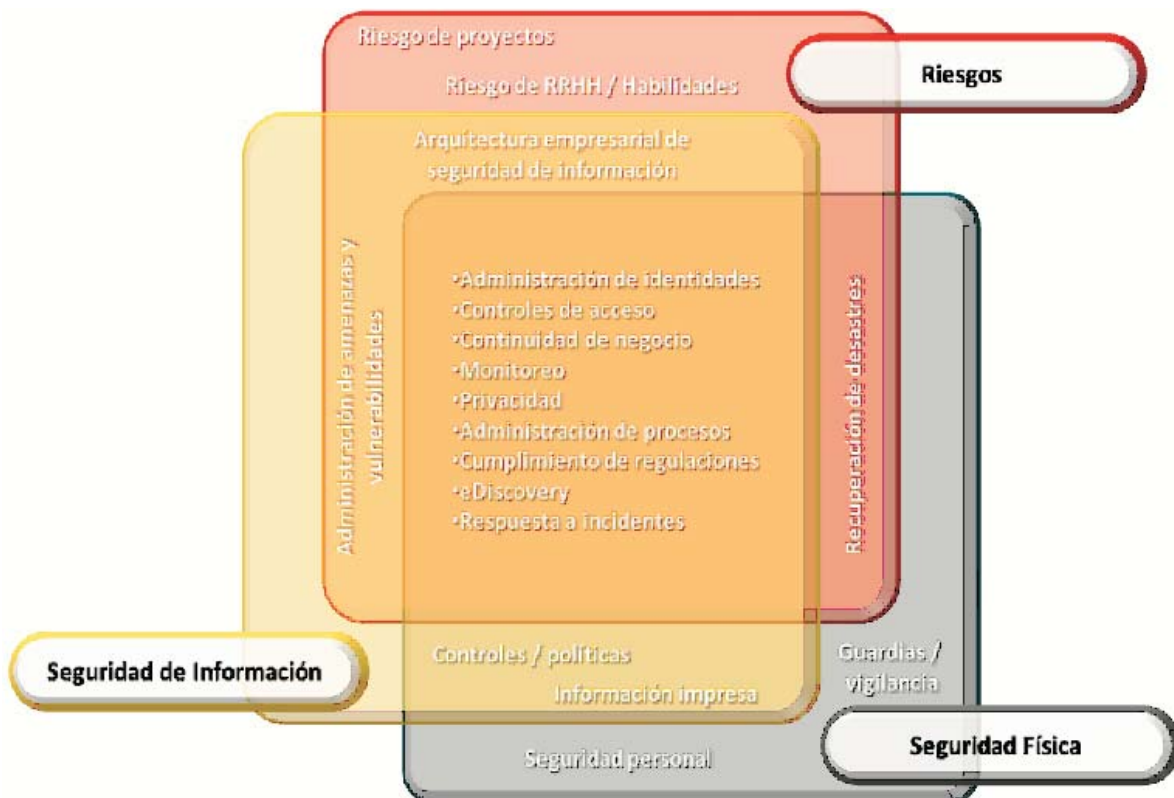
Use of the Active Directory system as the sole corporate management service for people both in electronic security systems and logical security access systems to the environment allows a perfect synchronisation to be established between both systems. Thanks to the synergy which is generated between both systems.

**Cerbero** in a compact, ergonomic terminal it incorporates a touch screen emulating a QWERTY keyboard, an intelligent card reading terminal and a biometric fingerprint terminal, all of which goes to form a robust, modern device with straight line design to complete the triple technology reader.

The efficiency and reliability of the system is maximised by allowing the management of data bases of users authorised and revoked dynamically as regards the active directory services.

**Cerbero** verifies and checks, once the user has been unequivocally identified from his/her biometric data compared with his/her digital signature and alphanumeric password providing access to the environment, being authorised to access the protected area.

The management of permission and privileges as regards access to an area becomes something as simple for the system administrator as the action of giving authorisation for the use of a printer or access permission to the files at a server. A sole management point and a sole environment further to the **synergy established between the Active Directory Service and the Access Control Service.**



## History

Since the first generation of Cerbero, the evolution has consisted of three vital aspects: increasing security, optimisation of the verification and integration times regarding new requirements within all physical security and logical security designs for an installation as critical as a CPD may be.

We can briefly distinguish between three major milestones in the evolution of Cerbero:

- **1st Generation:** the first generation of Cerbero developed by ACAL BFI IBERIA did not seem, on the outside, to be very different from a biometric terminal with a card and keyboard like so many others on the market. The basic difference was that in its interior there was a latest generation processor housing the functional procedure which connected its operation to the data base of the access control system and the active directory of the logical security system.
- **2nd Generation:** An idea soon came about as regards the first improvement in terms of using alphanumeric passwords instead of a numerical code. To this end, it became necessary to provide the terminal with a an expanded terminal which would allow the password to be entered in convenient fashion and which would not require the repetition of numerical keys as if it was a mobile phone. The current progress of the market as regards touch screens allowed this feature to be implemented.
- **3rd Generation:** having achieved system ergonomics and the time optimisation, the design of the surroundings was adapted in a terminal which was easy and convenient to use. Cerbero was provided with clear, simple usage instructions on the screen itself which allow the inexperienced user to unequivocally know the operation to be followed in the identification process required. **Cerbero 3rd Generation** had emerged as the maximum evolution of a highly tried and tested product and with the most robust, securest operating device on the market.



## Operation

In summarised diagram form we can represent the two access criteria (access of people and access to the environment) deployed by logical security and physical security systems and how **Cerbero** brings them together in a single environment.

With a view to carrying out user authentication under a single access control system, a system has been considered which complies with security specifications by way of three types of technologies (Fingerprint and digital signature) and digital password.

For authentication technologies based on fingerprints and digital fingerprints, user-related data is processed by way of the active directory of the client. The permission will thus be obtained for users by way of specialised consultation. Active directory data can be acquired by way of manual or automatic consultations (scheduled tasks).

The user-related data obtained from the active directory is restructured and entered in the access control system. The system will allow each user to have 11 credentials, 10 of them are connected with their fingerprints and the last credential is related with the electronic signature.



The data relating to fingerprints is stored on the reader and on the access management system data base.

In the access mode via a card with a certificate by way of ADPU and PDU commands, the reader distinguishes between certificate types

(X.509), checking whether the certificate has been issued by the anticipated entity. At the same time as the card is being processed (hash, SHA, MD5 ) the reader will open a dialogue screen where the alphanumeric password corresponding to the intelligent card will be entered. Whilst said password is entered, the reader checks whether the certificate in use has been revoked at the active directory.

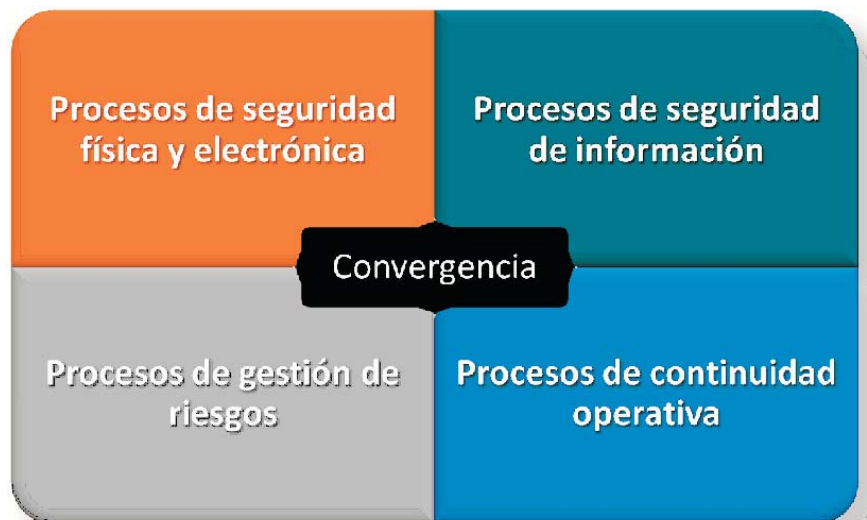
If the certificate has not been revoked by means of a request to the server, the "CLR" of the list of certificates revoked as well as the checking of the password entered, the reader will send the code relating to the user credential, allowing access to the protected area.

### Advantages and benefits

In the face of a globalised market in which the use of technology predominates as well as high criticality risks which generate major losses; the convergence between physical and logical security which **Cerbero** combines allows these events to be dealt with in accordance with synergy, efficiency and effectiveness schemes.

On the other hand, **Cerbero** allows major synergies geared towards the reduction in costs by dint of the use of technology, greater capacity for immediate reaction, optimising the preventive role and appropriate strategy operation.

The convergence between the logical and physical security of the **Cerbero** terminal allows an assurance of the operating continuity of the processes established in physical security in general and in particular in electronic security, but it also ensures the operating and methodological continuity of the security processes regarding information and it hugely simplifies risk management by merging in an absolutely inviolable identification environment the latest biometric and digital identification technologies.



All this has made Cerbero the ideal security solution for critical installations with a major integration nowadays in the design of physical and logical security systems in CPDs in our country.

## R&D Department

In 2005 ACAL BFI IBERIA started a new initiative in the field of research and development, creating the R&D Department. Geared towards improvement, we have provided our department with great human capital and great technical and innovative resources.

This structure transformed the company value proposal and it began to offer its installer clients a powerful global solution integrating the leading products in different technologies.

This is how IPNOVA was created, the integration platform under the umbrella of the state of the art. Fully developed and designed by ACAL BFI IBERIA to lend satisfaction to the requirements of each installer at each installation.

The gradual implementation of technological consulting at the different clients over time has given rise to the development of over 50 new products introduced onto the electronic security market such as that we have looked at in the present document.



C/ Anabel Segura 7 Planta de Acceso  
28108 - Alcobendas (Madrid)

Teléfono: 914531160  
Fax: 91 662 68 37

Innovación Española 