

Short Public Report
Application No. ULD090018

1. Name and version of the IT product or IT-based service:

Project's definition: Banco Guipuzcoano's internet banking platform for professional and corporate customers

Denomination: eBGempresa

Version: 2009.09.28.10.10

Logo: 

Url: <https://www.ebgempresa.com/>

2. Manufacturer of the IT product / Provider of the IT-based service:

Company Name: Banco Guipuzcoano, S.A.

Legal Address: Avenida de la Libertad, 21
20004 Donostia-San Sebastián (Spain)

Contact Person: Mr. Eduardo Goikoetxea Busto (Organization Manager)

Contact Address: Camino de Portuetxe, 35
20018 Donostia-San Sebastián (Spain)

Telephone: +34 943418435

Email: egoikoet@bancogui.com

3. Time frame of evaluation

2009 March – 2009 December

4. EuroPriSe Experts who evaluated the IT product or IT-based service:

Technical Experts: Luis Alfaro, Judith Larreta

Legal Expert: Santiago Alfaro

Company: Sigacus Gestión, S.L.

Address: Plaza Azkoitia, 5, 2º D
20011 Donostia-San Sebastián (Spain)

Telephone: +34 943453588

Email: sigacus@sigacus.com

5. Certification Body:

Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein
Holstenstraße 98 24103 Kiel

Tel +49-431-988-1283, Fax -1223
<http://www.datenschutzzentrum.de>
www.european-privacy-seal.eu

6. Specification of Target of Evaluation (ToE):

Target of Evaluation for eBGempresa includes:

- Contracting the service. Professionals & corporative customers must sign a basic banking services contract (“General conditions”) and an internet banking contract before using eBGempresa.
- eBGempresa interface. Users navigate and operate through the different screens of the web site. Hereby, personal data of users are processed. This processing must be compliant with EuroPriSe requirements. It must be respectful with users’ privacy and data security. eBGempresa offers users some of the services they can do at the branches.
- Data subjects rights. Users are data subjects and they can ask for the exercise of their rights.

Target of Evaluation ends when:

- users link from eBGempresa to other web sites
- users sign electronically (ToE legally ends because the transaction is finished; technically the user can remain connected and use eBGempresa, generate more transactions, etc.)
- users log out
- users shut the internet browser down

Out of Target of Evaluation:

- general banking operative resulting from users transactions performed on the platform: e.g. bank internal processing of payments and collections, transfers, cards, trading, etc., each one with its own specific regulation, both national and international
- possible data transmission to different kinds of recipients (banking service receivers, other correspondent banks and financial companies, control authorities, etc.) both national and international
- access by special digital certificate issued and provided by the Bank (this access system has fallen in absolute disuse and it will be disabled by the Bank in March 2010)
- Spanish Electronic National Identification Document (issued and managed by the Spanish Ministry of Interior)
- Banco Guipuzcoano's intermediate systems
- hosting and other services provided by a processor
- links to other Banco Guipuzcoano's web sites (eBGempresa Broker, BG Infotar, EBGempresa)
- links to services provided by other companies, as well as the services themselves
- internet connections and public networks provided by third parties
- users' hardware and software equipments

7. General description of the IT product or IT-based service:

eBGempresa - Banco Guipuzcoano's internet banking platform for professional and corporative customers is a banking service channel that offers users some of the services they do at the bank's branches. It is an additional and complementary service, provided by Banco Guipuzcoano. Online banking access is voluntary.

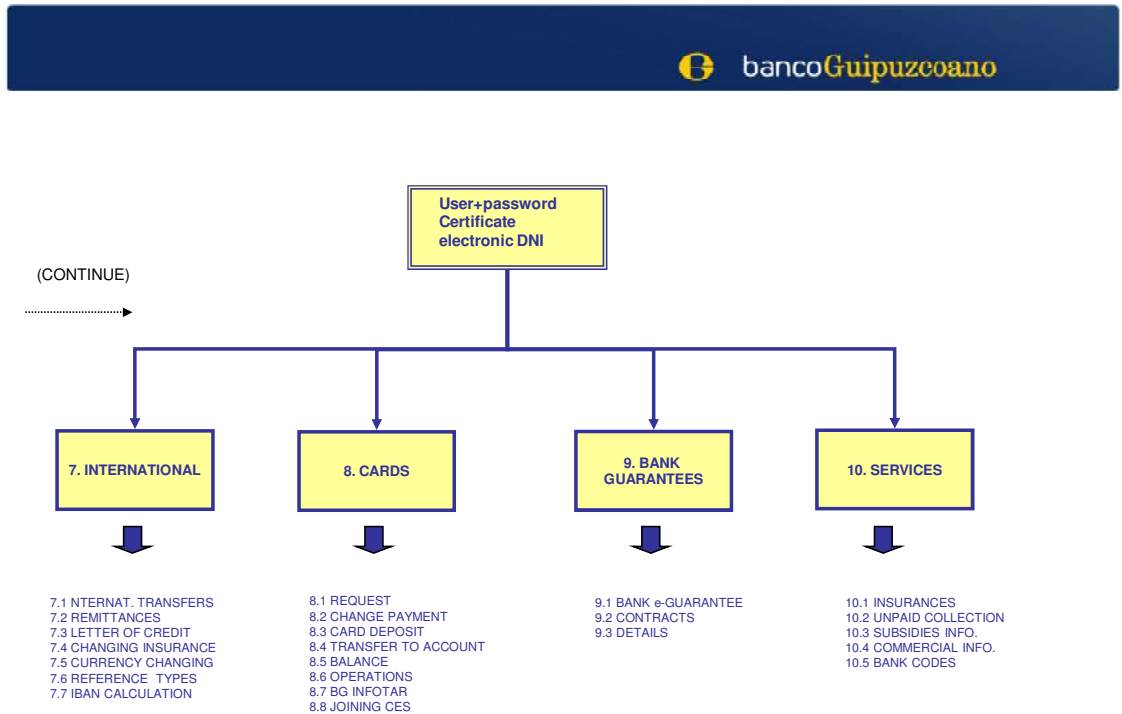
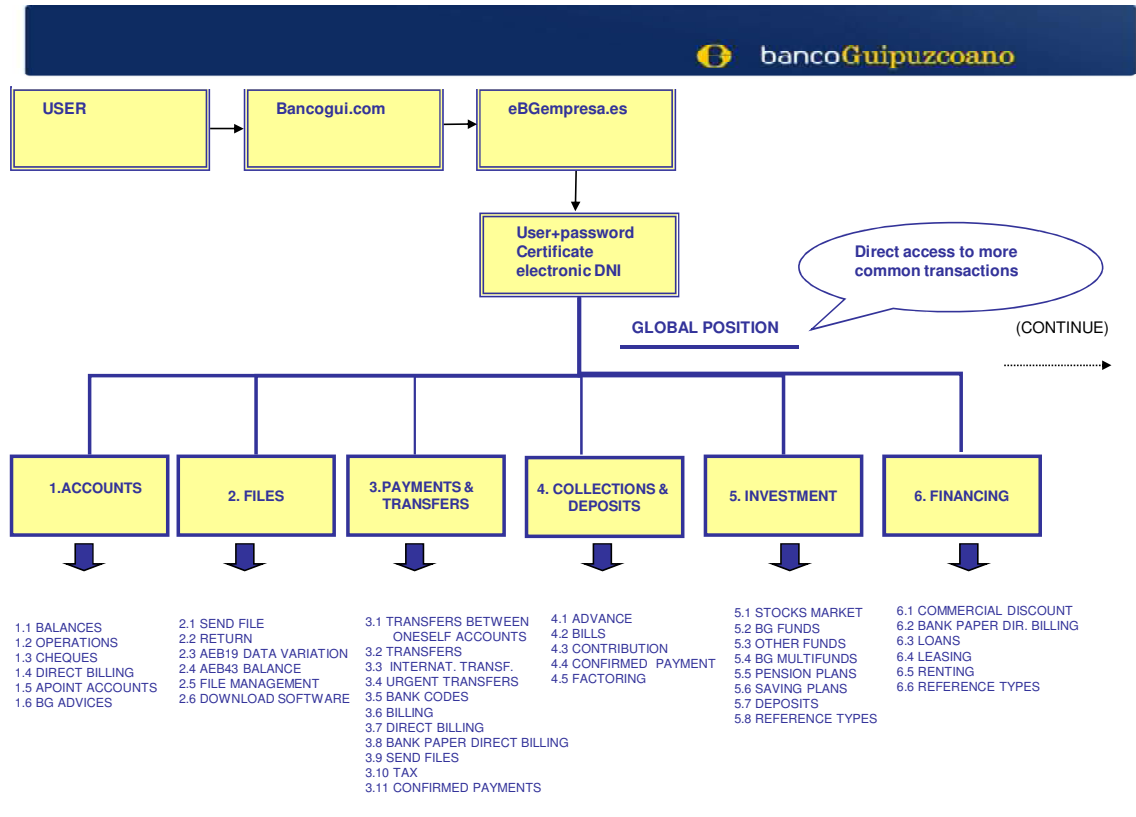
eBGempresa users are Banco Guipuzcoano traditional banking services users. Banco Guipuzcoano customers interested in this additional service must request it at the branches, where qualified staff informs them. Before accessing eBGempresa customers must sign a written contract.

Once they get authorized access to eBGempresa, users can access eBGempresa web site (<https://www.ebgempresa.com/>) using their codes.

Access to eBGempresa can be done using different methods (three): username and password (provided by the bank), digital certificate (issued and provided by the bank; fallen into disuse and to be cancelled in March 2010) or Electronic National Identity Document (provided by the Spanish Government).

Users accessing eBGempresa visualize a menu that allows them to execute different operations. eBGempresa provides plenty of financial services, like checking account balances, fund transferences, managing payments, collections and deposits, requesting credit cards and controlling operations made with them, trading stocks, trading investment funds and pension plans, requesting information about loans, leasing and other financial products, etc.

eBGempresa Web Map:



8. Transnational issues:

The service is offered only in Spain and there are no transnational operating bodies or entities.

9. Tools used by the manufacturer of the IT product / provider of the IT-based service:

Web Servers:

IBM xSerie 445/3650

Red Hat Enterprise Linux ES Release 4

Operative platforms: Java and Websphere application server

Software development languages: Java (server), Html and JavaScript (client)

Hosts:

IBM 2064

Operating System Z/OS

DataBase Manager DB/2

Resource Access Control Facility

10. Version of EuroPriSe Criteria for Experts used for the evaluation:

EuroPriSe Criteria Catalogue - Version 1.0

11. Evaluation results:

eBGempresa is an **online banking service** that Banco Guipuzcoano offers its professionals and corporative customers. The Platform is an **additional** banking service channel, it is not an independent bank and it has no exclusive functions. There are no customers who are only online banking customers (all customers have an assigned office). eBGempresa is restricted to the Bank's pre-existing customers. It is an additional banking tool, different from the office or telephone banking.

eBGempresa offers users some of the services, as described above, they do in the office. They can check their account balances, order payments, transfers, etc. The eBGempresa "Web Platform" is our Target of Evaluation (ToE).

eBGempresa is **restricted** to customers who have **contracted** its service. Banco Guipuzcoano has a strong vocation for guarantying data protection and it has the personal data processing authorizations demanded by law. This information is shown clearly and visible in the contracts customers must sign: "Basic Contract" and "Internet Banking Contract". In these contracts, that customers must read, accept and sign, data subjects are informed expressly, among other things, about controller's

identity, purposes of the processing, personal data protection, rights of access and of rectification of their data and possible recipients of the data. Contracts also inform about the necessity to record the IP address, in order to avoid fraudulent use of the service. Besides, when users contract the service, their adviser staff explains them the operative and the service's possibilities, the way they should use the different online services, different codes management and basic security measures. Staff also explains the meaning of the different clauses of the contract and the meaning of signing contract's sheet of signatures. At this point users must indicate if they want to receive advertising information. It is remarkable that Banco Guipuzcoano does not use direct marketing means. The bank can edit brochures in paper and send them (by postal mail) to the customers who have previously asked for it. Later on users can refuse the processing of their data (e.g. for advertising purposes) at any moment executing the rights established in 95/46/EC Directive.

Customers can also retrieve all this information at the Bank's **official web site**, selecting the following options: Legal Advice, Privacy Statement and Security Advice.

To access eBGempresa (the private area of Banco Guipuzcoano web site) customers need to **identify** and **authenticate**. They can do that using username and password codes, digital certificate (issued and provided by the bank; fallen into disuse and to be turned off in March 2010) or Electronic National Identity Document (provided by the Spanish Government). When using user name and password codes length required is between 6 and 8 characters (system distinguishes between upper and lower levels and "ñ" character is also accepted), although using 8 character passwords is recommendable. It must be noticed that all bank customers are informed about personal codes usage in the contracts and at the web site.

Banco Guipuzcoano does not only inform customers, but all its **employees**. All the employees are trained on personal data protection and attendance to a course about the subject is compulsory. Bank provides them with different documentation about the subject, that can be consulted in all Banco Guipuzcoano's offices (printed documentation available) or accessing the corporative web site.

Banco Guipuzcoano's eBGempresa service is based on **transparency** principles as service itself shows, offering a complete demo version available before becoming a customer, an interactive helping system available at every screen, web maps, etc.

Data processed by the bank are hosted in a Data Centre owned by the **Processor**. Data Centre has strong physical and logical security measures. Contract between Controller and Processor is in line with Article 17(2)-(4) of the 95/46/EC Directive.

Accessing and using eBGempresa services involves personal data processing. eBGempresa processes both primary and secondary data.

Primary data processed can be classified in:

- Identification data: Full name, tax identification number, delivery and tax address, e-mail address, telephone number
- Electronic signature and access data: username and password
- Data derived from banking operative: all the different operations user can done using the online platform

Secondary data processed are:

- Cookies
- IP address
- Channel traffic data: statistical data related to use of access channel

When users access eBGempresa a transaction is registered. Any type of operation users do is memorized in the “Electronic Diary” as different transactions. Transaction includes all processing data. For example in a balance checking, a transaction will be registered, but this transaction will not record the content of the balance, only the fact, that the user has charged his or her balance data (but not the data themselves). Transaction includes operations with consequences for eBGempresa as well as operations with no banking consequences, as checking balance (just reading), accessing the website (identification and authentication) etc. eBGempresa stores all the transactions related to the data subjects. Registered information is needed to carry out the services requested by users and it is necessary to guarantee the legal security of the transactions. Security and the operative purposes require registering and storing information that identifies data subjects.

Electronic Diary **transactions** are registered at the host. They remain at a “legible” status for a maximum period of 2 months (can be shorter). This period is due to technical reasons. Then they are transformed to a **not legible** status, not accessible. They cannot be technically processed. They are removed from the Data Base. They are not located at the same hard disks than the other data. They are not accessible from the system. They are not available for Bank’s operators, customers, etc. They are excluded from regular processing. This is an automated process. It converts all the transactions. No transaction is left behind.

If these data must be recovered, the Bank must execute established specific recovery processes. Data remain at this not legible status for six years, according to specific legislation (Art. 30 Spanish Code of Commerce), that establishes that companies must keep books, correspondence, documentation and receipts concerning their business, for six years. Transactions, compulsory kept, are needed for **law compliance**. These data are not processed or used for other purposes.

Legal obligations of keeping these data involve compulsorily keeping data subjects’ personal data, including IP address used for connecting to the platform. Therefore, the **Bank expressly informs** customers in the Online Banking Contract, that the Bank can record the IP address of the computer used to perform the transaction so that it may be used as evidence of the source of the transaction and in order to **prevent fraud**.

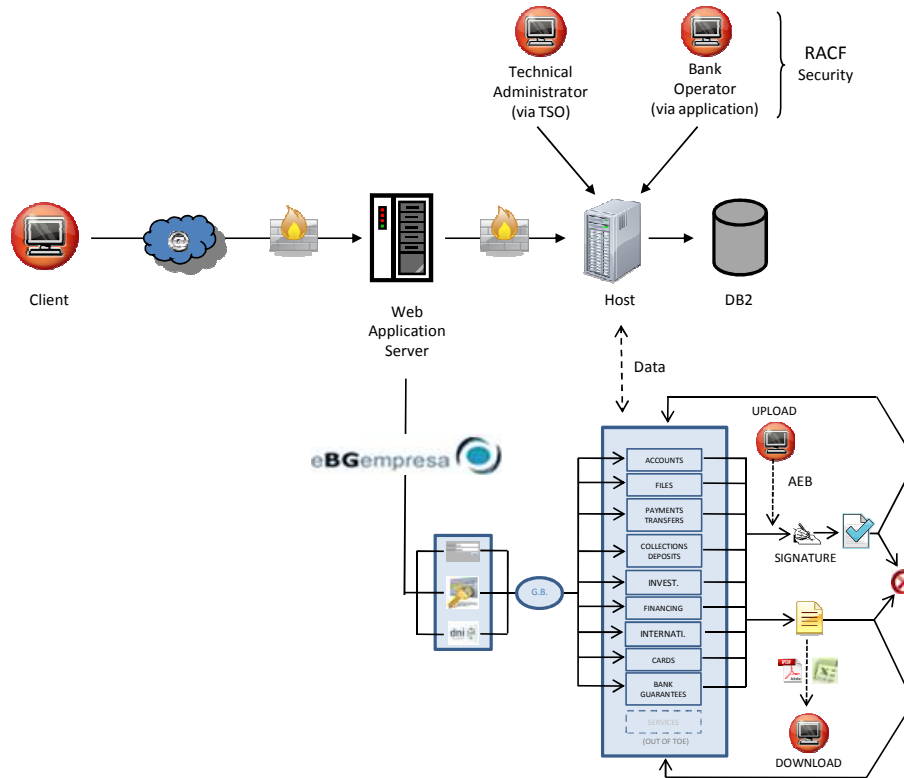
Data contained in the Electronic Diary can be used for **statistical purposes**. Electronic Diary data can be studied to analyze globally (not personally, not individually) total number of transactions, used channel and type of operation. The Bank only analyzes totals and percentages of utilization of the different available operational channels. The purpose of these statistics is technical: to know how many transactions and the channel used for them, in order to assign the necessary resources for each one. Once statistic analysis has been done, data are definitely **deleted** after 18 months.

All information processed or transferred by networks is encrypted using https: 128 bits **encryption** protocol, using VeriSign SSL certificates (an internet security standard used by many banking entities). Digital certificates are protected by cryptographic techniques and guarantee a safe connection.

12. Data flow:

Data Flow Image

eBGempresa Data Flow:



13. Privacy-enhancing functionalities:

Banco Guipuzcoano has implemented accurate procedures and strong technical measures to ensure personal data security and data subjects' privacy in its online banking service for Companies and Professionals: eBGempresa.

Contracts for eBGempresa and Web Site Privacy Statement provide detailed information on privacy relevant issues in a transparent way.

14. Issues demanding special user attention:

Users should make use of the possibility to choose a password containing 8 or more digits including special characters.

15. Compensation of weaknesses:

-Not applicable-

16. Decision table on relevant requirements:

<i>EuroPriSe Requirement</i>	<i>Decision</i>	<i>Remarks</i>
Data Avoidance and Minimisation	Adequate	Service collects only data necessary to carry out the service and in compliance with legal obligations
Transparency	Excellent	eBGempresa service´s information and contracts are complete and easily understandable
Technical-Organisational Measures	Excellent	Excellent physical access measures, adequate identification and authentication logical measures
Data Subjects' Rights	Adequate	eBGempresa informs about users rights and forms are available in all Banco Guipuzcoano branches

Experts' Statement

We affirm that the above-named IT product / IT-based service has been evaluated according to the EuroPriSe Criteria, Rules and Principles and that the findings as described above are the result of this evaluation.



SAN SEBASTIAN
2009/12/17

SANTIAGO ALFARO

Place, date

Name of Legal Expert

Signature of Legal Expert



SAN SEBASTIAN
2009/12/17

LUIS ALFARO

Place, date

Name of Technical Expert

Signature of Technical Expert



SAN SEBASTIAN
2009/12/17

JUDITH LARRETA

Place, date

Name of Technical Expert

Signature of Technical Expert

Certification Result

The above-named IT product / IT-based service passed the EuroPriSe evaluation. It is certified that the above-named IT product / IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data security.

Place, date

Name of Certification Body

Signature