Short Public Report

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

BGNetPlus: Banco Guipuzcoano´s internet banking for customers

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

Company Name: Banco Guipuzcoano, S.A.

Address: Avda. de la Libertad, 21, 20004 Donostia-San Sebastián (Spain)

Contact Person: Eduardo Goikoetxea Busto (Organization Manager)

3. Time frame of evaluation:

From 2008/03/14 to 2008/11/07

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

Name of the Legal Expert: Santiago Alfaro (Sigacus Gestión, S.L.)

Address: J.M. Salaberria 43, 9 20010 Donostia-San Sebastián (Spain)

Name of the Technical Expert: Luis Alfaro (Sigacus Gestión, S.L.)

Address: J.M. Salaberria 43, 9 20010 Donostia-San Sebastián (Spain)

5. Certification Body:

Name: Unabhängiges Landeszentrum für Datenschutz (ULD)

Address: Holstenstr.98 D - 24103 Kiel Germany

6. Specification of Target of Evaluation (ToE):

The Target of Evaluation includes **Banco Guipuzcoano´s online banking services** for individual customers, also known as **BGNetPlus** (www.bancogui.com and www.bgnetplus.com). The Platform is a banking service channel that offers users some of the services they do in the office, as checking account balance, asking for chequebooks, making a transfer, requesting a credit card and controlling operations made with it, purchasing/selling stocks, checking purchased stocks´ status and modifying them, contracting investment funds and pension plans, requesting information about loans, leasing and renting.

In order to generate the service, a procedure is necessary that guides the customer-users. This procedure, known as "interface" is our Target of Evaluation. Target of Evaluation finishes when customer signs electronically.

ToE does not include:

- general banking operatives resulting from users transactions performed on the platform: e.g. bank internal processing of payments and collections, transfers, cards, insurances, 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 insurance companies, control authorities, etc.) both national and international
- Bank´s intermediate systems
- hosting services by a processor
- internet connections and public networks provided by third parties
- users´ hardware and software equipments (just take into consideration express advices Bank gives to customers)

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

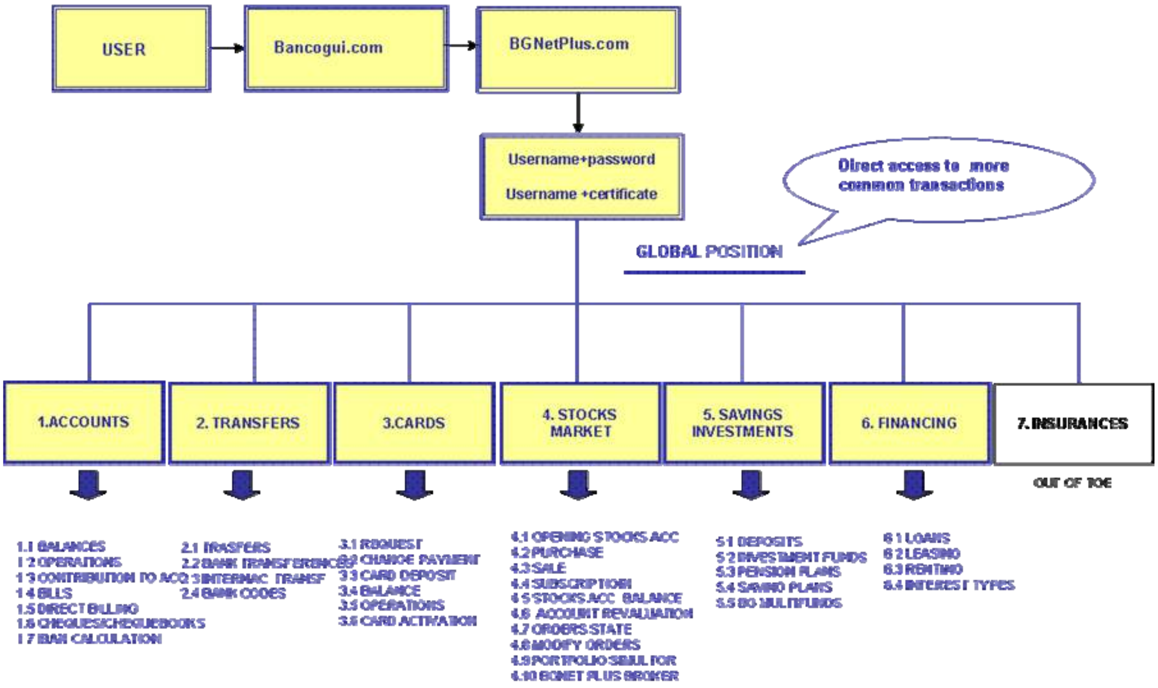
BGNetPlus online banking service is an **additional service** provided by Banco Guipuzcoano. Online banking access is voluntary and **complementary** to traditional office activity.

BGNetPlus users are Banco Guipuzcoano traditional banking users. Banco Guipuzcoano´s customer interested in this additional service must **request** it at the office, where qualified staff inform them. Before accessing BGNetPlus customers must sign a **written contract**.

Once they get BGNetPlus access authorization users must access Banco Guipuzcoano web site public area and use **identification and authentication** provided codes to access private area, that is it, BGNetPlus.

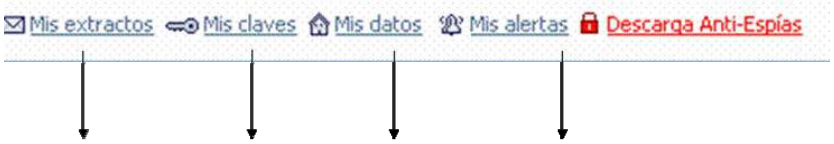
Users visualize a menu that allows them to execute different **operations**: check account balance, ask for chequebooks, make a tranfer, request a credit card and control operations made with it, purchase/sale stocks, check purchased stocks´ status and modify them, contract investment funds and pension plans, request information about loans, leasing and renting, etc. All transactions are definitive and instantaneously executed.

Web Map



Direct access from Global Position

OPTIONS AVAILABLE FROM ANY SCREEN



Statement checking

Password modifying

Address checking, modifying

OUT OF TOE

8. Transnational issues:

The service is offered in Spain only 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 Server:
IBM xSerie 445/3650
Red Hat Enterprise Linux ES Release 4
Operative platforms: Java and Websphere application server
Software development languages: Java (server), Hmtl and JavaScript (client)
Safelayer

Host:
IBM 2064
Operating System Z/OS
DataBase Manager DB/2
Resource Access Control Facility

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

Europrise Criteria Catalogue for Experts (Version 0.3)

11. Evaluation results:

BGNetPlus is an **online banking service** that Banco Guipuzcoano offers its 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). BGNetPlus is restricted to the Bank´s pre-existing customers. It is an additional banking tool, different from the office or telephone banking.

BGNetPlus offers users some of the services, as described above, they do in the office. They can check their economic situation, order payments, transfers, etc. and in order to generate the service, it is necessary a procedure that guides the customer-users. This procedure, known as “Web Platform” is our Target of Evaluation (ToE).

BGNetPlus is **restricted** to customers who have **contracted** its service in one of Banco Guipuzcoano offices. Banco Guipuzcoano has a strong vocation for guaranting 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. Contratcs 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, wich is always done at the office, their adviser staff explain them the operative and the service´s possibilities.

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 BGNetPlus (the private area of Banco Guipuzcoano web site) customers need **identification** and **authentication** codes they receive they sign the contract.

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 BGNetPlus 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.

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

Primary data processed can be classified in:

- Indentification data (Delivery address, Tax address, E-mail)
- Electronic signature and access data (Username, Password, Digital Signature)
- Data derived from banking operative (Balances, Accounts operations, Accounts, Payment by standing over, Transfers, Transferences, Card, Stocks, Funds)

S**econdary data** processed are:

- Cookies
- IP adress
- Channel traffic data

When users access BGNetPlus 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 BGNetPlus as well as operations with no banking consequences, as checking balance (just reading), accessing the website (identification and authentication) etc. BGNetPlus 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 to register and store information that identify data subjects.

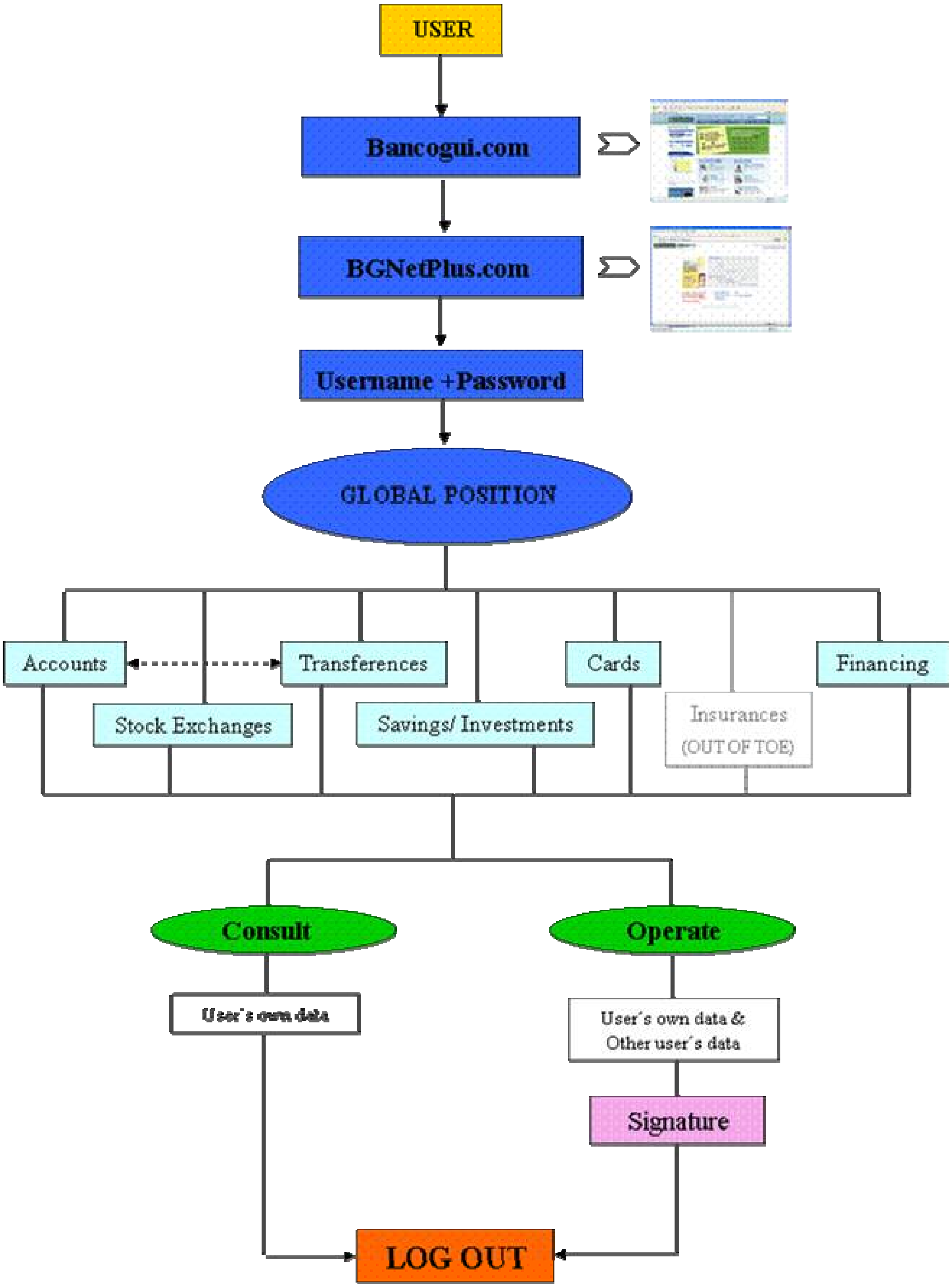
Electronic Diary **transactions** are registered at the host. They remain at a "legible" status for a maximum period of 2 months (can be shorter). Then they are converted to a **non-legible**, non-accessible situation and can not be technically processed any longer. If these data must be recovered, the Bank needs to establish 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 involves 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, section 4.7, 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 have 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:


USER
Bancogui.com
BGNetPlus.com
Username +Password
GLOBAL POSITION
Accounts
Transferences
Cards
Financing
Stock Exchanges
Savings/ Investments
Insurances
(OUT OF TOE)
Consult
Operate
User´s own data
User´s own data &
Other user´s data
Signature
LOG OUT

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 individuals: BGNetPlus.

Contracts for BGNetPlus 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:

16. Decision table on relevant requirements:

EuroPriSe Requirement	***Decision***	***Remarks***
Data Avoidance and Minimisation	Adequate	Service collects data necessary to comply with legal obligations.
Transparency	Excellent	BGNetPlus service´s information and contracts are complete and easily understable
Technical-Organisational Measures	Excellent	Strong physical access measures, efficient identification and authentication logical measures
Data Subjects’ Rights	Adequate	BGNetPlus 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 SANTIAGO ALFARO

2008-11-07

Place, date Name of Legal Expert Signature of Legal Expert

SAN SEBASTIAN LUIS ALFARO

2008-11-07

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