






SECURITY CONCEPT FOR BKMS® SYSTEM

Business Keeper AG (BKAG) provides their clients with systems for the recording and examination of anonymous reports of whistleblowers. The patented and certified Business Keeper Monitoring System (BKMS® System) represents a procedure for the sustainable prevention of and fight against fraud and infringements of legal, ethical and company-internal norms. Reports on diverse subject matters may be recorded.

The BKMS® System is used as an anonymous communication platform from the side of the whistleblower (employee of companies and administration or citizens) for the making of anonymous reports. At the same time the examiner (compliance officers, corruption agents, ombudsmen, audits and examinations within the company or administration) receives the report and can enter into an anonymous dialogue with the whistleblower via this platform.

Die application of the BKMS® System includes the following services:

-  Usage of the web and application server
-  Continuous updating of the application
-  Access security
-  Data protection
-  User support within business hours of BKAG



The usage of software via the internet as ASP concept (Application Service Providing) will not only technologically complement the application possibilities for companies and public administration in the future but also considerably reduce economic costs. On average these costs are written off after 1.3 years (survey of IDC, SevenOne Media and NFO Infratest 2003). The BKMS® System has therefore been designed on an ASP-basis. Investments for computer programs, hardware, updates, internal networks, maintenance and IT specialized staff will significantly be reduced.

An important precondition for the implementation of ASP concepts includes the protection from unauthorized access to data which will be explained in the following.

Certificate

The certificate has been issued by a publicly appointed and sworn expert for the first time on July 16, 2004. Object of examination included an extensive physical and program-specific analysis proving the security of the system and of the used servers. The certificate has continuously been updated.

In detail, the certificate confirms that:

-  the whistleblower's anonymity is protected,
-  the reports cannot be decrypted or interpreted by a third party including Business Keeper AG.

Translation:**Markus Müller, Master degree in Computer Science (Diplom-Informatiker)
Public appointed and sworn surveyor**

By the chamber of commerce and industry of North Rhine-Westphalia
For data processing systems and applications in the field of telecommunication, especially internet

Certificate

The signee certifies herewith for the company

**Business Keeper AG
Bayreuther Str. 35**

10789 Berlin

on the basis of the technically analyzed version of the Business Keeper Monitoring Systems and its applied server on December 15th, 2010,

that the anonymity of the whistleblower is protected and that with the usage of secure passwords neither the company Business Keeper AG nor third parties may, with a realistic effort, decrypt or interpret the reports.

The analysis applies to the software version with the following checksum of the encryption module:

bkwebsecurity.jar

MD5:

1b1e6b43804bea0170f30cf9c02fcc45

SHA-256:

bd4570f7bb1e2171c246dac7a137e395988c2bde55c85e16b8e986e091e83495

This certificate is based upon the results stated in the expert's report **G11 0228 1**. The certificate is no longer valid if either the logging characteristics or the encryption module is changed.

48308 Senden, on March 1st, 2011

Markus Müller
Master degree in Computer Science (Diplom-Informatiker)
Surveyor

Physical Security

The application of the BKMS® System is implemented on dedicated servers in a high-level security location in which, for instance, the European Central Bank also secures its data and servers. A current SAS 70 Report Germany 2008 is available for the data centre. The internet platform is integrated in the existing national and international networks and has broadband connections to the most important cross-points worldwide.

The reliability of the server in the high security centre is ensured by an automatic recognition of hardware dysfunctions within the server network. The administration and maintenance of the server is the responsibility of the Business Keeper AG IT staff. Access to the system necessary at elimination of a hardware fault is being enabled by specialists of the high security centre only upon approval of BKAG. An interpretation of reports through BKAG or the maintenance team is not possible by any means.

Access and Data Transfer

The high security data centre is secured by an actively controlled firewall. Only the services needed for the application and maintenance are installed on the server. A transfer started from the inner or a direct access to the server is not possible. This way, it is secured that no activation of data transfer may be executed through an unauthorized third party.

With a third security level the databank is secured through a firewall that only responds to requests from the local system. The security measures are updated continuously.

An annual penetration test is carried out for quality assurance purposes.

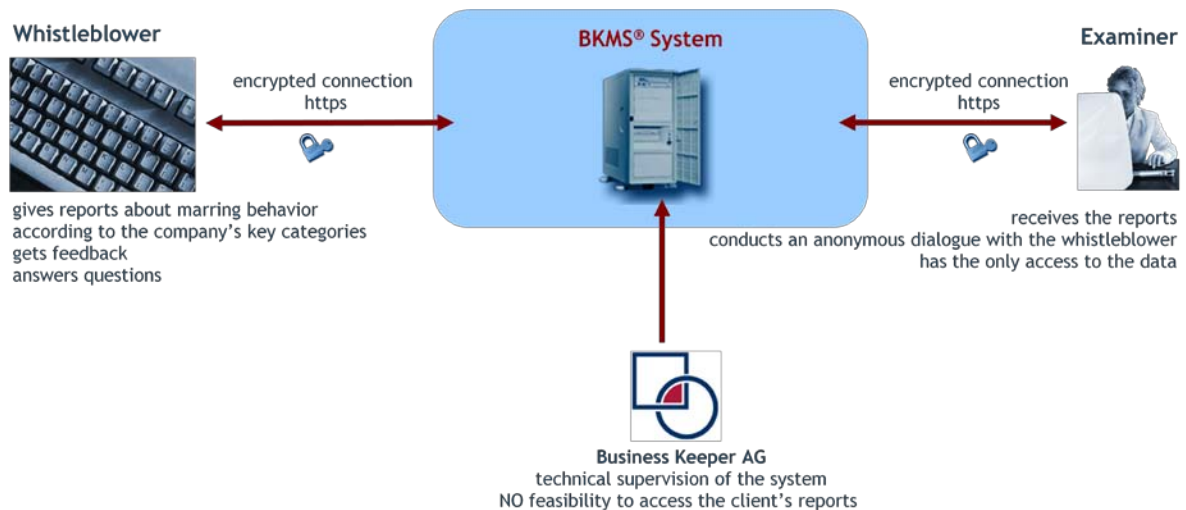


Figure 2: Security Concept BKMS® System

The transfer of data from the whistleblower to the server, as well as from the examiner to the server, is carried out by means of a standard encryption https. Direct communication between the whistleblower and the examiner is not possible via this path. BKAG uses a standard encryption for the pure transfer of data. The security of the transfer of encrypted data is being ensured through the applied standard encryption and does not call for separate technique. This encryption is also applied by banks and organisations, which transfer highly confidential data.

All connections of BKAG to the server system for system maintenance and data protection are conducted via SSH.

Protection against Automatic Assaults – Security Code

A security question is used as a means of protection from automated attacks. The application generates, with the help of a random generator, an alphanumeric character sequence that is integrated into a graphic system.

Before entering into the report making and accordingly the examination process, the number-letter combination has to be manually inserted.

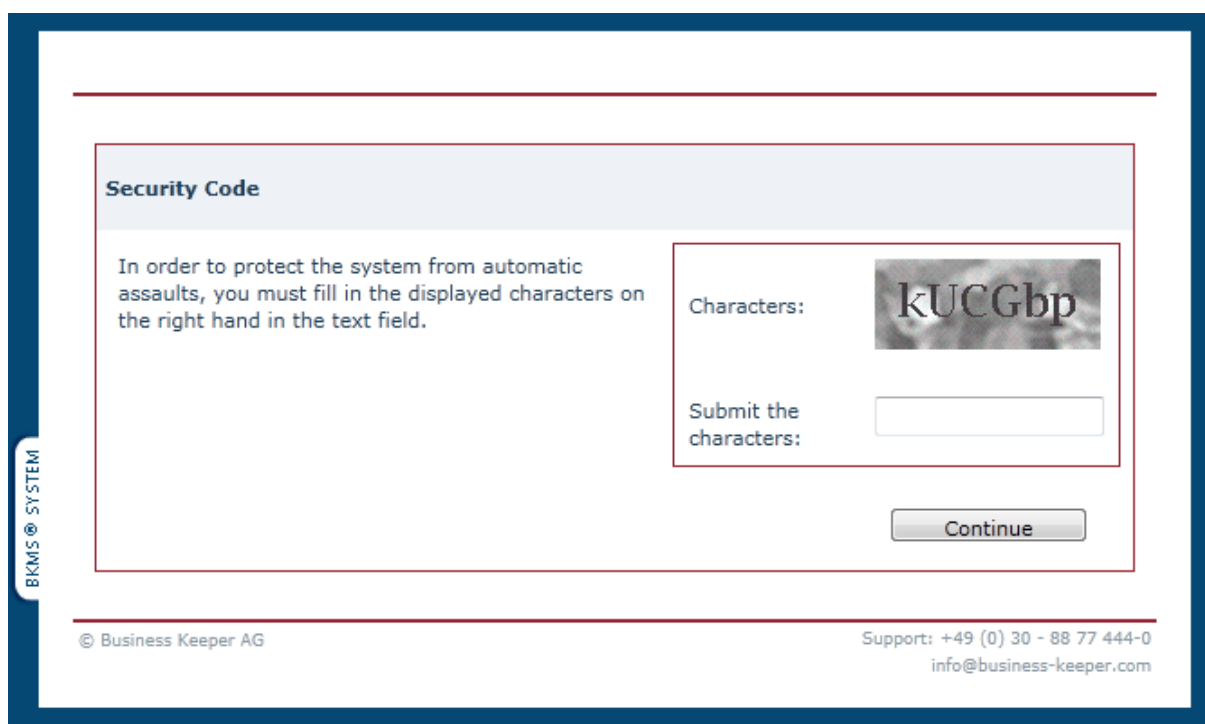


Figure 2: Security Code BKMS® System






The web server has a registered server certificate with which a clear cut secure legitimization may be ensured. This way it is guaranteed that all reports and correspondences are conducted via a clear-cut SSL-connection.

Anonymous Platform and Report Data

When developing the communication platform, it was highest priority to ensure anonymity to the whistleblower and to protect the system from unauthorized access of a third party.







The protection of anonymity is guaranteed by a multi-level registering process including pseudonym and password. With the help of an individual encryption, report data, postbox data and examination data are being protected from unauthorized access of a third party. Only the authorized examiner may interpret data. The security system refuses unauthorized examiners from access.

This way, the following is ensured:

-  A report may only be read by the authorized examiner the report was sent to.
-  The whistleblower remains anonymous and may nevertheless communicate with the examiner via the postbox.
-  The postbox set up by the whistleblower may only be accessed by the whistleblower himself.
-  A third party may neither interpret report data of the client nor reports in the postbox
-  Reports of a client account may not be interpreted by BKAG.

Responsibility of security of the client

The security of client data is guaranteed when it is adhered to the following action:

-  The responsible client-contact person receives access data to their client account on the server from BKAG.
-  With these access data the client may sign in as Systemadministrator (Sysadm).
-  The Sysadm should immediately change access data for the respective client account. This way it is secured that only the client may access the system. After changing the access data no third party including BKAG may access the client account.
-  After the Sysadm has changed the password, the client has become responsible for the use of the account.
-  After again signing in, the Sysadm generates a client-specific security code (DataPIN). This code is to be kept confidential.
-  Thereafter, the contractually agreed number of examiners will be set up by the Sysadm and activated according to level of authorization, responsibility for report nature and general entitlement.

Responsibility of security from the side of the whistleblower

The anonymity of the whistleblower may only be guaranteed when the whistleblower refuses from revealing or attaching personal data of any kind within his report.

Data Protection

Data protection is conducted on a daily basis to an internal server of BKAG via an SSH-connection. SSH is a secure, standardized encrypted connection for the transfer of data.

The data protection allows for report and examiner data which may have accidentally been deleted by the client to be recreated on the server. The encrypted data may hence be decrypted, read and interpreted by the client by the use of his individual authorization rights and access data. The security concept allows BKAG at no time to interpret the data in any way.

The security concept of BKAG, its techniques and procedure, represent the currently highest possible standard for the recording of a report and the leading of a dialogue and the expertise is being continuously updated to the newest standards.