



ProCredit Bank

Macedonia

ProCredit Bank, Head Office bul. Jane Sandanski 109a, 1000 Skopje, Macedonia

(Annex 1)

Tender Announcement

Procurer:	ProCredit Bank AD Skopje, Republic of Macedonia
Name of tender:	Tender for supplying of Security Information and Event Management (SIEM) Solution
Number of tender:	13/2009
e-mail:	tenders@procreditbank.com.mk
Fax:	(02) 321 99 01

Date of announcement of tender: 20.02.2009

Final date for sending of offers: 05.03.2009

Dear Sirs,

ProCredit Bank AD Skopje is going to make a selection of company for Security Information and Event Management (SIEM) solution for below systems and database.

Item	OS and DB description	Approximately Qty.
1.	MS Windows Server 2003/2008 standard edtn. 32 and 64 bit	50
2.	MS SQL Server 2000/2005 standard edtn.	2
3.	MS Exchange Server 2003/2007 standard edtn.	1
4.	Check Point FW Cluster – Linux (SecurePlatform) (Management)	1
5.	IPS/IDS - ISS proventia G100	2
5.2.	IPS/IDS – ISS Server Sensor for MS Windows Server 2003	3
6.	MS ISA Server 2006 Standard edtn.	1
7.	Cisco Routers and switches	50
8.	PIX firewall	1

The price should be expressed in EUR with all included costs (travelling expenses, VAT, import duty etc) f-co to the Head Office of ProCredit Bank in Skopje, respectively ready to use.

The SIEM solution need to be complete solution including:

- Software (licenses, console, interfaces, agents...);
- Hardware (server, storage for logs, backup of old logs, ...);
- Depends of the licensing model, yearly maintains fee
- Implementation, configuration and maintains of the solution
- Service Level options and appropriate response time
- Training course

ProCredit Bank
bul. Jane Sandanski 109a
1000 Skopje, Macedonia
S.W.I.F.T.: PRBUMK22

Phone +389 /02/ 321 99 00
Fax +389 /02/ 321 99 01
www.procreditbank.com.mk
info@procreditbank.com.mk

Members of the Managing Board:
Jovanka Joleska Popovska
Valentina Trajceva Nikovska
Emilija Spirovska
Deputy General Manager
Carina Dunker





ProCredit Bank, Head Office bul. Jane Sandanski 109a, 1000 Skopje, Macedonia

Proposed solution must meet or exceed the following specifications. Suppliers should confirm whether the solution meet the Questions and Requirements requested by placing a tick (yes, not or n/a) in the relevant box, also supplier should the place page number of their proposal for answers description. Questions with opt are optional.

Item		Question / Requirement	Answer Yes/No	Descriptive answers (page number)
Security and Risk Management				
1.	Compliance			
1.1		Which of the following compliance standards are taken account of within the product:		
1.2	opt	Sarbanes-Oxley		
1.3	opt	Payment Card Industry Data Security Standards		
1.4	opt	Health Insurance Portability and Accountability Act		
1.5	opt	Gramm-Leach-Bliley Act		
1.6		other:		
1.7		Can the product map individual security policies and show their compliance status?		
2.	Function			
2.1		In which of the following formats can reports be generated:		
2.2		html		
2.3		pdf		
2.4		xml		
2.5		csv		
2.6		other:		
2.7		In which of the following ways can reports be accessed or made available:		
2.8		Email		
2.9		GUI		
2.10		Web-GUI		
2.11		other:		
2.12		Can the privacy of users be protected by anonymization or pseudonymization?		
2.13		Is it possible to map the business criticality of certain assets in the product?		
Technical Functions				
3.	Architecture			
3.1		Which database is used/supported?		





ProCredit Bank

Macedonia

ProCredit Bank, Head Office bul. Jane Sandanski 109a, 1000 Skopje, Macedonia

3.2		Does the system make compression of the data in database? If yes specify the compression ratio.		
3.3		Does the product use agent-based collectors to collect logs?		
3.4		Is the system multi-client capable?		
3.5		Is it possible to build distributed installations (e.g. worldwide or for scalability)?		
3.6		Does the product have the ability to reflect hierarchical structures in distributed environments, e.g. one correlator in Bitola, one correlator in the Strumica and one to govern those two?		
3.7		Is the system-internal communication authenticated and encrypted? If so, by which encryption algorithms and schemes, at which stages?		
3.8		Does the system internal communication occur over single, well-defined TCP-ports? Which ports?		
3.9		Does the event processing occur in real time?		
3.10		Do correlation, analysis, and alarming occur in real time?		
4.		Supported Platforms		
4.1		Supported platforms for the collector?		
4.2		Supported platforms for the correlator?		
4.3		Supported platforms for the database?		
4.4		Supported hardware? Intel- and AMD-processors?		
5.		Collector Features		
5.1		Can logs from the following source types get imported?		
5.2		Cisco PIX		
5.3		Cisco Routers		
5.6		Cisco Catalyst Switches		
5.7	opt	Symantec Endpoint Protection 11.0		
5.8	opt	Symantec Mail Security 7.61		
5.9	opt	Aladdin Token Management System		
5.10		Windows XP/Vista		
5.11		Windows Server 2003/2008		
5.12		Microsoft ISA Server 2006		
5.13		Microsoft Exchange Server 2003/2007		
5.14		Microsoft SQL Server 2000/2005		
5.15	opt	Avaya IP 406 System		
5.16		Check Point		
5.17		Internet Security System		
5.18		Explain how database auditing work. Does it need additional permission for the collector? How the solution ensure that the auditing of the database is in place and does it alert if auditing is stopped?		
5.19		Is there a way to import and correlate non-standard application logs (e.g. mainframe logs, individual applications)? How and what general conditions do apply to log format?		

ProCredit Bank
bul. Jane Sandanski 109a
1000 Skopje, Macedonia
S.W.I.F.T.: PRBUMK22

Phone +389 /02/ 321 99 00
Fax +389 /02/ 321 99 01
www.procreditbank.com.mk
info@procreditbank.com.mk

Members of the Managing Board:
Jovanka Joleska Popovska
Valentina Trajceva Nikovska
Emilija Spirovska
Deputy General Manager
Carina Dunker





ProCredit Bank

Macedonia

ProCredit Bank, Head Office bul. Jane Sandanski 109a, 1000 Skopje, Macedonia

5.20		What restrictions apply to format and size of log events?		
5.21		Are syslog and SNMP supported mechanisms to collect logs?		
5.22		Apart from syslog and SNMP which methods do exist to import logs? (E.g. logs via local files, named pipes, database queries)		
5.23		Is the log collector capable of caching logs in case of network problems or outage of the correlator service?		
5.24		What forms of normalization are done at the collector level?		
6.		Filtering, Aggregation, Correlation, Prioritization		
6.1		On which levels can events be filtered out? (Collector, correlator, database)		
6.2		How can filters be configured?		
6.3		Which event data fields are available? How many data fields are there?		
6.4		Can similar events be aggregated into one? By which criteria can this be arranged?		
6.5		What can be the outcome of a correlation of single events (e.g. new event, alert, create incident)?		
6.6		Does the product support statistical correlation?		
6.7		Is the product able to discover attack patterns (low and slow attacks, zero day attacks)?		
6.8		Are events automatically prioritized by the system?		
6.9		What factors are considered during the prioritization process?		
6.10		Can the prioritization process be customized?		
6.11		Can historical data be replayed, e.g. for forensic analysis or for testing of new correlations?		
6.12		Is the traceability of the history of an event at the end of its lifecycle guaranteed?		
6.13		Let's assume, a hacker is attacking several systems, one after another. Is it possible to easily and automatically become aware of the hacker's actions?		
6.14		Is it possible to similarly track normal user behavior which involves several independent systems?		
7.		Assets, Vulnerabilities, Modeling		
7.1		Does the product support modeling of assets?		
7.2		Which asset properties are configurable? (e.g. name, IP-address, known vulnerabilities, location, customer)		
7.3		By which properties can assets be grouped/organized together?		
7.4		Which interfaces for modeling assets and keeping them up-to-date are provided by the product to avoid entering them manually?		
7.5		From which vulnerability scanners can scanning data be imported:		
7.6		Internet Security System		

ProCredit Bank
bul. Jane Sandanski 109a
1000 Skopje, Macedonia
S.W.I.F.T.: PRBUMK22

Phone +389 /02/ 321 99 00
Fax +389 /02/ 321 99 01
www.procreditbank.com.mk
info@procreditbank.com.mk

Members of the Managing Board:
Jovanka Joleska Popovska
Valentina Trajceva Nikovska
Emilija Spirovska
Deputy General Manager
Carina Dunker





ProCredit Bank

Macedonia

ProCredit Bank, Head Office bul. Jane Sandanski 109a, 1000 Skopje, Macedonia

7.7		other:		
7.8		Do default correlation rules come with the product? How many and what can be achieved with these (examples only)?		
7.9		Can correlation rules keep their function when assets properties or events (e.g. because of a log source change) referenced by these rules become updated?		
8.	Sizing, Scalability, Performance			
8.1		What is the maximum number of Events per Second per correlator-database system? Remark: Vendors please assume the biggest possible (and reasonable) hardware platform.		
8.2		What is a typical time frame, for which events can be evaluated in near real-time (i.e. event data is still "online"), e.g for reports, forensic analysis? (E.g. 1 month)		
8.3		What is the usual way for the product to cope with a sporadically occurring huge EPS rate (e.g. a DOS-attack, worm-outbreak)?		
8.4		What is the required bandwidth for collecting logs via WAN?		
8.5		If the solution needs installation of agent - client, how many resources (RAM, processor, Disk load etc) does it use in real-time processing?		
8.6		If the solution needs installation of agent – client, how does it affect the performance of SQL Server?		
9.	Integration			
9.1		With which 3rd party tools does the product integrate itself for incident management (e.g. trouble ticketing)?		
9.2		How can system response times, processing times and system load be collected by 3rd party monitoring systems (e.g. Nagios, HP Open View, EMC Smarts)?		
9.3		Which other system values are available for 3rd party monitoring systems? Which interfaces are being offered towards these monitoring systems?		
9.4		For system-users: Which 3rd party authentication or authentication mechanisms (LDAP, AD, RADIUS) are supported?		
9.5		Which of the following alerting mechanism are supported: GUI, Email, SMS/Pager, 3rd party tools?		
		Can the data in the database be accessed directly?		
10	Usability			
10.1		Is there a Web-GUI?		
10.2		Is there a GUI being not web-based (e.g. a console)?		

ProCredit Bank
bul. Jane Sandanski 109a
1000 Skopje, Macedonia
S.W.I.F.T.: PRBUMK22

Phone +389 /02/ 321 99 00
Fax +389 /02/ 321 99 01
www.procreditbank.com.mk
info@procreditbank.com.mk

Members of the Managing Board:
Jovanka Joleska Popovska
Valentina Trajceva Nikovska
Emilija Spirovska
Deputy General Manager
Carina Dunker





ProCredit Bank

Macedonia

ProCredit Bank, Head Office bul. Jane Sandanski 109a, 1000 Skopje, Macedonia

10.3		If there are both a Web- and a non-Web-GUI: Are there any restrictions to the functionality of one of them? Which restrictions?		
10.4		If there is a Web-GUI: What web server is used/supported?		
10.5		Can the GUI be configured to reflect different access levels and complexity?		
10.6		Does the system provide a change auditing function to keep track of configuration changes?		
10.7		Can access rights be configured at the following levels: -system areas -system functions -user group?		
10.8		Is there an internal knowledgebase to share know-how among system-users?		
10.9		Does the GUI provide visualization of event flow or of associated systems?		
11	High Availability			
11.1		Is there High Availability for the collector?		
11.2		Is there High Availability for the correlator?		
11.3		Is there High Availability for the database?		
11.4		Modularity: How would the sudden failure of a log source impact the whole system? (with/without HA)		
11.5		Modularity: How would the sudden failure of a collector impact the whole system? (with/without HA)		
11.6		Modularity: How would the sudden failure of a correlator impact the whole system? (with/without HA)		
11.7		Modularity: How would the sudden failure of a database impact the whole system? (with/without HA)		
12	Operational aspects			
12.1		Can collected log data automatically be handled and archived (e.g. automatic backup of database partitions)?		
12.2		What repeating operational tasks concerning the database are unavoidable?		
12.3		Is there a built-in case-management?		
12.4		Does the system monitor the status of its own components, e.g. the collectors' and the database's status?		
12.5		Can the system be backup during operations?		
13. Support, Trainings				
13.1		Direct or Channel Support?		
13.2		7x24 Support?		
13.3		Support languages?		
13.4		Support locations?		

ProCredit Bank
bul. Jane Sandanski 109a
1000 Skopje, Macedonia
S.W.I.F.T.: PRBUMK22

Phone +389 /02/ 321 99 00
Fax +389 /02/ 321 99 01
www.procreditbank.com.mk
info@procreditbank.com.mk

Members of the Managing Board:
Jovanka Joleska Popovska
Valentina Trajceva Nikovska
Emilija Spirovska
Deputy General Manager
Carina Dunker





ProCredit Bank

Macedonia

ProCredit Bank, Head Office bul. Jane Sandanski 109a, 1000 Skopje, Macedonia

13.5		# of support personnel in total?		
13.6		# of support personnel in Europe?		
13.7		# of support personnel in Macedonia?		
13.8		Is remote access support available?		
13.9		Does the company offer regular trainings on the product?		
13.10		Is there a partner program?		
13.11		Is there a certification program for the product?		
14. Vendor - Strategic Evaluation				
14.1		List reference installations in Macedonia! Characterize them by Events per Second or Events per Day, if possible!		
14.2		List reference installations in Europe! Characterize them by Events per Second or Events per Day, if possible!		
14.3		Awards and Tests: List the awards won by the product and describe the achieved scores and ranks in tests!		
15.Licensing				
15.1		Does the product keep on working if the license expires?		
15.2		Which product components will need to be activated by a license?		
15.3		Describe the licensing model and levels of the licenses!		
15.4		We would need a 45 days evaluation license without costs. Pilot installation with full functionality for 3 (or to be specified) systems. Can the company provide this?		

Form and contents of the offer:

1. The offer is prepared in written form
2. The offer should contain:
 - a. Name, address and place of residence of the Bidder, telephone numbers and fax numbers, e-mail addresses and contact persons;
 - b. Price of the bid, with separately calculated VAT. The price should be expressed in EUR;
 - c. Manner of payment;
 - d. Delivery date;
 - e. Warranty;
 - f. Evidence of quality (certificate of quality, technical characteristics, technical specifications, functional characteristics, esthetic characteristics, etc);
 - g. Reference List
 - h. Certificate of solvency issued by the Central Registry;
 - i. Current status issued by the Central Registry;
 - j. Court certificate, stating that bankruptcy or liquidation procedure has not been initiated;
 - k. Certificate stating that the measurement for restriction of performing an activity has not been imposed on the company;
 - l. Signed and sealed anti-corruption statement;

ProCredit Bank
bul. Jane Sandanski 109a
1000 Skopje, Macedonia
S.W.I.F.T.: PRBUMK22

Phone +389 /02/ 321 99 00
Fax +389 /02/ 321 99 01
www.procreditbank.com.mk
info@procreditbank.com.mk

Members of the Managing Board:
Jovanka Joleska Popovska
Valentina Trajceva Nikovska
Emilija Spirovska
Deputy General Manager
Carina Dunker





ProCredit Bank

Macedonia

ProCredit Bank, Head Office bul. Jane Sandanski 109a, 1000 Skopje, Macedonia

m. In case a foreign legal or physical entity is a bidder, he submits an audit report from the legal entity issued by a renowned audit house;

n. Copy of valid ID card or passport for physical person.

The documents are submitted in original form or copies and should not be older than 6 (six) months.

The offer and the documents should be written in Macedonian or English Language.

The following criteria shall be applied during the selection of the supplier:

- price.....75 points
- warranty and maintenance.....10 points
- quality and realization of projects....10 points
- cooperation with the bank.....5 points

The selected suppliers are obliged to open accounts in ProCredit Bank AD Skopje.

They should be sent in closed envelope, labeled "Do not open" and "For tender" to the below given address:

**Str. Jane Sandanski 109a,
1000 Skopje,
Republic of Macedonia**

Labeled Tender for supplying of Security information and Event Management (SIEM) Solution Nr.13/2009.

The offers which have arrived by e-mail or fax, offers that have arrived after the period has expired shall not be considered valid during the deciding upon the tender.

The envelope must not contain any label thereby the submitter can be identified.

If upon request of ProCredit Bank, the Bidder is required to prepare a template of the subject of the bid, the preparation is on the Bidder and the model remains in the ownership of the Bidder. ProCredit Bank is not obliged to compensate the costs for preparation of the template and is not obliged to buy it.

*ProCredit Bank
bul. Jane Sandanski 109a
1000 Skopje, Macedonia
S.W.I.F.T.: PRBUMK22*

*Phone +389 /02/ 321 99 00
Fax +389 /02/ 321 99 01
www.procreditbank.com.mk
info@procreditbank.com.mk*

*Members of the Managing Board:
Jovanka Joleska Popovska
Valentina Trajceva Nikovska
Emilija Spirovska
Deputy General Manager
Carina Dunker*

