Deloitte
Statsautoriseret Revisionsaktieselskab
CVR-nr. 24 21 37 14

Weidekampsgade 6
Postboks 1600
0900 København C

Telefon 36 10 20 30
Telefax 36 10 20 40

www.deloitte.dk

25.04.2006

Giritech A/S
Att.: Jens Tiedemann
Herstedøstervej 27-29 C2
2620 Albertslund

Report on agreed-upon procedures regarding security features in Giritech's G/On product

Introduction

Giritech A/S (hereafter Giritech) has made an agreement with Deloitte Enterprise Risk Services (hereafter ERS) to perform agreed-upon procedures regarding security features of G/On. Our work was performed according to the Audit standard ISA4400.

This report describes the result of the test we performed in accordance with the agreed-upon procedures between Giritech and ERS related to the G/On versions described below.

Our report is intended to be used by Giritech itself and for distribution to Giritech's existing and potential customers.

G/On version

The G/On solution consists of a number of software modules which have different version numbers. There are several components for the client as well as the server. The tables below summarize the list of components and relevant version that have been tested by Deloitte. All these components together make up G/On Version 3.1.0.0 which was released on October 28th, 2005.

Client

Component	Description	Version	Source
G/On USB	USB Key version of the G/On client	3.1.0.0 (E3 SR1)	Giritech/EClient.exe
G/On Desktop	Windows application version of the G/On client	3.1.0.0 (E3 SR1)	C:\Program Files\GOnDesktop\EClient.exe

Server

Component	Description	Version	Source
EMCADS Core	The patented core of the G/On Server Software	3	Provided by Giritech
G/On USB Server Token	USB Key with needed to obtain license and for server and management tools to operate	1.0.0.0	UD-rom\UD-Logo.exe
G/On Server	G/On Server application	3.1.0.0 (E3 SR1)	C:\Program Files\Emcads\Emcads.exe
G/On Builder	G/On Server installation and initial configuration	3.1.0.0 (E3 SR1)	C:\Program Files\Emcads\GOnBuilder.exe
AccessRules Manager	Zone, rule and EDC manager	3.1.0.0 (E3 SR1)	C:\Program Files\Emcads\CxRulesAdmin.exe
G/On Admin	G/On Menu and user manager	3.1.0.157 (E3 SR1)	C:\Program Files\Emcads\GonAdmin.exe
USync	Tool for copying groups and users from the AD	3.1.0.0 (E3 SR1)	C:\Program Files\Emcads\USync.exe

Scope

Our report is documented in a structured report with defined test procedures that are reproduceable in order to provide a test suite that can be used to ensure that future releases comply with Giritech's expectations.

The tests have been performed according to the test plan which has been agreed upon with Giritech.

The test has been performed on the set-up at Deloitte which consists of a G/On EMCADS server, 1 G/On USB server key, and 5 G/On USB client keys.

The test procedures have focused on tests that Giritech believe will support the following 7 statements defined by Giritech:

1. G/On provides true two factor authentication (adapted EDC and user name/password) to obtain access.

2. Copying the software from an USB key or Desktop does not provide access from the new device – even if proper user id/password is given.
3. G/On provides strong (163-bit ECC) encryption, both in establishing a connection and in the subsequent (256-bit AES) application connectivity.
4. The EDC is not able to perform any actions without having been authenticated by the G/On server (EDC contains no intelligence).
5. G/On provides mutual authentication of both the client to the server – and authentication of the server to the client (preventing phishing/pharming).
6. G/On only enables application connectivity – not network connectivity.
7. The G/On administrator has full control of the applications that the G/On client can access.

Test and report

For each of the 7 statements, the following table gives a summary of the test procedures and the test results.

Statement 1
G/On provide true two factor authentication (adopted EDC and user name/password) to obtain access.
Test procedures and results
Data sniffing in relation to session establishment Data has been sniffed during session establishment and analyzed to find weaknesses that could compromise the authentication mechanism. All data in session establishment were found to be encrypted or encoded. **Access to the EMCADS server from third party utilizing Remote Desktop** It was tested whether it was possible to utilize remote desktop to a client computer with an active G/On USB client and thereby gain access to the EMCADS server. It is not possible to access the EMCADS server through an active G/On connection utilizing Remote Desktop if the security recommendations from Giritech are implemented, since the client will be properly firewalled.

Statement 2

Copying the software from an USB key or Desktop does not provide access from the new device – even if proper user id/password is given.

Test procedures and results

Collect usable information from the G/On USB key in an attempt to circumvent the use of USB key
The content of the key has been investigated before and after initialization. Also the hardware manufacturer's home page has been searched in order to copy or by other means circumvent the use of the USB key.

No usable information has been found on the key, and no weaknesses have been discovered that could be used to copy the G/On USB client or by other means circumvent the two factor authentication provided by the G/On USB client.

Copy the G/On Desktop to another host and establish connection to the server
The G/On Desktop client was copied from one client computer to another to see if there is an effective copy protection.
If the G/On Desktop client is copied from one client computer to another, our test shows that it will not be functional on the client computer to which it is copied.

Install the soft client on VMware and copy the VMware server image to another host and establish connection
The G/On Desktop client was installed in a VMware image. Once the desktop client was adopted by the EMCADS server and the G/On Desktop client was functional, the VMware image was copied to another client computer.

Utilizing VMware it is possible to copy the G/On Desktop client from one client computer to another, and it will be functional on both client computers.

Statement 3

G/On provides strong (163-bit ECC) encryption, both in establishing connection and in the subsequent (256-bit AES) application connectivity.

Test procedures and results

Test of the communication between G/On client and EMCADS server and attempt to trick unencrypted traffic

To test the communication, we have performed a man-in-the-middle attack and monitored traffic between the G/On client and server. There are some observations regarding recognizable patterns, but no useable information or weaknesses have been found in the communication.

Data were found to be encrypted or encoded, and there is no plain text information travelling between the server and client during communication.

Initial registration is encrypted

We have analyzed traffic during the initial registration by performing a man-in-the-middle attack and sniff all traffic.

The initial registration seems to be encrypted or encoded.

Statement 4

The EDC (EMCADS Data Carrier) is not able to perform any actions without having been authenticated by the G/On server (EDC contains no intelligence).

Test procedures and results

Test of the communication with the G/On client in order to make the client accept unauthorized data.

A man-in-the-middle attack was set up between the client and server, and data was injected to the client in order to make the client accept unauthorized data.

During our test it was not possible to make the client accept unauthorized data.

Statement 5

G/On provides mutual authentication of both the client to the server – and authentication of the server to the client (preventing phishing/farming).

Test procedures and results

Session hijacking and man-in-the-middle attacks

To be able to do session hijacking and man-in-the-middle attacks it was tested whether it was possible to manipulate data to the server.

During our test it was not possible to manipulate data travelling to the server, since the connection or session is closed if data is changed.

Simulation of EMCADS server in order to do a replay attack

A replay attack depends on weak authentication. To test whether there are weaknesses in the authentication mechanism in the G/On solution, the protocol has been analyzed. Since everything is encrypted or encoded, it is not possible to thoroughly test the authentication scheme. However, our analysis shows that the traffic is alternating for each connection.

It does not seem possible to emulate the EMCADS server, since there are no traffic patterns that are constant between connections.

Statement 6

G/On only enables application connectivity – not network connectivity.

Test procedures and results

Establish a session and attempt to break out or escalate privileges

A G/On USB client session has been created for one application, and it has been attempted to tunnel (embedded communication channel) another application through the connection. We have found no ways to escalate privileges or manipulate user status.

It has not been possible to tunnel other applications through an application specific G/On session.

Statement 7
The G/On administrator has full control of the applications that the G/On client can access.
Test procedures and results
Attempt to gain access to other menus or applications than initially provided To access other menus or applications than provided by the administrator, we have attempted to launch applications that were not part of the menu and tunnel them through an active session. This was not possible as described in statement 6. We have also observed that the menus according to the log file are downloaded from the server each time the G/On client is started. It has not been possible to gain access to other menus or applications than those originally provided.

Limitations

The specific test tools and methodology have been chosen by Deloitte and agreed to by Giritech.

Per definition (ISA 4400) agreed-upon procedures provide no assurance for a conclusion whereas an audit provide a high degree of assurance and a review provides a moderate degree of assurance for a conclusion. Therefore, Deloitte makes no conclusion that the results of the tests verify the above statements 1 - 7, and we do not express any degree of assurance on the security features of G/On. If further test procedures had been performed, other findings may have been found and been reported.

The lack of public documentation regarding the client/server interaction has made it difficult to plan tests to target the encryption scheme.

There are some technical aspects of testing that have not been included in the scope of the test, partly due to time constraints. These include:

- Code review.
- In-depth crypto analysis.
- Tests that require modification or development of hardware.
- In depth application analysis including reverse engineering.

Deloitte
Statsautoriseret Revisionsaktieselskab

Knut Gotfredsen
State Authorised Public Accountant, CISA