

Giritech New Product Announcement

G/On™ 5

Tuesday, October 20, 2009.

Giritech A/S proudly announces:

G/On 5 – The new Secure Virtual Access platform from Giritech

G/On 5 is an entirely new, significantly more powerful generation of Giritech's G/On product line for secure remote application access. G/On 5 supports **Windows, Mac, and Linux** clients, new **smart-card based authentication** devices and methods, improved performance, and a wealth of features such as integrated support for Citrix, MS Terminal Server, LDAP, MS AD, Wake-on-LAN, and a new and more robust user interface for administration and management.

G/On 5 provides a platform for all of an organization's needs for connecting remote and local users from *any device* from *anywhere* across *any network* to give users secure access to their applications, their office PC or their virtual desktop. As a completely new and innovative security technology G/On 5 also includes an option for the user to boot up a remote PC with a **G/On Secure Desktop** that runs G/On from a managed and protected Linux operating system directly from the G/On USB authentication device.

G/On 5 is a fully integrated solution for managing **security, connectivity, users, devices, and applications**. In a single, simplified product, G/On 5 delivers **two-factor Authentication, Authorization, FIPS 140-2 encrypted Data Confidentiality, Integrity** and **Virtual Connectivity** - innovatively different from traditional VPNs and SSL-VPNs. Together with its Single Point of Management, G/On 5 offers dramatic cost savings in establishing, managing, supporting, and auditing secure access for all employees, external contractors, and business partners.

G/On 5 is built on a new software platform that has been developed using industry standard and leading edge software tools and technologies to ensure support for current and future needs and challenges. The platform is based on an open architecture with well-defined interfaces and plug-ins, allowing continuous integration of new technologies and functionality.

Availability

G/On 5 is available immediately for new customers.

Existing G/On 3.x customers can upgrade now to G/On 5 to provide secure remote access for Mac and Linux users or otherwise take advantage of the new G/On 5 Authentication Tokens included with this announcement. Read more about the expected availability of support for the current G/On USB H2 and H3 keys used for G/On 3.x on page 16.

The New G/On 5 Client

G/On 5 introduces a new, more flexible and diverse client concept. In addition to supporting different operating system platforms, the G/On 5 Client will be able to support a wide range of **authentication tokens**. These tokens vary significantly in functionality and capabilities and G/On 5 provides different client options offering customers the benefit of the various features and price points. For instance, one of the options is a variety of tokens which offer smart card functionality combined with or integrated with other functionality. Most are USB based tokens combined with memory for software storage and CD-ROM and some of them have integrated hardware encryption and additional smart card readers. Future plans for G/On 5 include support for more traditional tokens such as the RSA token, SMS-based tokens, and other One Time Password (OTP) devices.

G/On 5's new, flexible plug-in architecture is designed to support these and future new and innovative authentication tokens. Over time, this will enable the development of add-ons for specialized solutions incorporating features and functions of different tokens and token-based solutions. One example is the creation of completely integrated G/On based solutions for physical access (door access control) and virtual access (IT access) based on smart card and contactless tokens.

G/On 5 Solution Scenarios

In one single product, G/On 5 offers secure access solutions to a variety of infrastructures that would otherwise require dedicated products at high cost. Typical G/On 5 solutions include:

- Use of employee's own PC at home to get secure access from home to the desktop of their office PC. As no other products are needed and G/On 5 provides Wake-on-LAN capability this solution is the most cost effective and energy saving secure remote access solution available.
- Many companies have a virtual desktop infrastructure like Citrix, MS Terminal Server or VMWare and users are typically also offered access to these through G/On. Using G/On for secure access offers the added benefit that companies are not limited to only one virtual environment. G/On gives users a single, simple interface to any mix of these virtual environments thus providing organizations more choice and flexibility without the added cost of handling different infrastructures.
- For quick access to e-mail, order entry, sales numbers or company Intranets, users are also offered direct access to specific applications.
- For people travelling – without a PC – G/On 5's USB devices offer access from almost any PC to a virtual desktop, specific applications and/or to their office PC.
- For employees with a company laptop, G/On 5 users are also provided secure access to client/server applications like Outlook, allowing employees to access mail and their

personal folders on their laptop. Most client/server applications can be enabled in G/On but without the need for the traditional VPN infrastructure.

- The new G/On 5 microSD based authentication option can be integrated into most USB based broad band modems giving broad band connectivity and authentication in one single device. Most laptops come with integrated broad band modems and some of these also feature ports for the G/On 5 microSD card making the laptop a very convenient G/On device.
- G/On 5 controls precisely what users have access to and which features they have available. For instance, user access can be configured to prevent users from file upload/download, copy/paste and local print to avoid data mistakenly leaving the corporate network.
- Some organizations only allow access from PC's they know and manage. This is very costly as it requires the organization to provide laptops to each employee. G/On 5 now offers a cost effective alternative via the G/On Secure Desktop. This option enables the user to boot the remote PC from the G/On USB device and run G/On via a company managed image of a Linux operating system without using the operating system and hard disk of the remote PC.
- G/On 5 gives the organization a single point of management of all access and its detailed logging of data traffic provides documentation.
- In public and semi-public environments like schools, colleges, universities, libraries and the like, G/On 5 can be used to offer managed Internet access for students using their own PC's while they and their teachers can have secure access to very specific resources on the network.

The Power and Value of G/On 5

The objective of G/On 5 is first and foremost to offer organizations the opportunity to achieve significant cost savings by providing **highly secure access** for employees, external contractors, and business partners. G/On 5 offers an *unprecedented* combination of security, flexibility, ease of use, ease of deployment, and ease of management. Cost savings are achieved through the significant simplification of IT infrastructure allowed by G/On 5 compared to traditional solutions in the market place.

G/On 5 can be implemented to provide value for small and large organizations and for organizations looking for a simple remote access solution. In other implementations, G/On 5 leverages its optional features to satisfy even the highest level of security and regulatory compliance. This includes the requirements of local, state and federal government, police, and security agencies as well as certain departments within the military.

As an integral part of this objective, G/On 5 addresses the issue of handling the multiplicity of new devices being brought to the market. New Windows, Mac and Linux operating systems are becoming increasingly popular with users who tend to expect that they will be able to use these devices, not only for their personal, private use, but also for professional work use. This trend imposes increasing challenges for IT administrators to enable connectivity from devices and operating systems not supported by the employer.

In those situations where remote work is mandated to be done from a known and managed environment, the new G/On Secure Desktop provides the option to boot the remote PC from a fully integrated version of a Linux operating system that runs G/On.

A critical function of G/On 5 is its policy based management tools which enable IT, business, and security administrators to focus on the business objectives of providing users access to applications while being assured that their G/On based infrastructure implements, enforces and documents company policies and regulatory requirements.

The remaining sections of this product announcement document give more details on the G/On 5 technology and the features and benefits of deploying G/On. Please visit www.giritech.com for additional information about G/On.

Content

G/On 5 – The new Secure Virtual Access platform from Giritech	1
Availability	1
The New G/On 5 Client	2
G/On 5 Solution Scenarios	2
The Power and Value of G/On 5.....	3
G/On 5 Feature Overview	6
Background.....	7
Innovating G/On: Version 5 Architecture and Technology	8
G/On 5 Solution Components.....	8
The G/On Server	10
The G/On Client	14
The G/On Secure Desktop	14
New G/On 5 Authentication Tokens.....	15
G/On 5 Hardware Authentication Tokens available today:.....	15
Planned G/On 5 Hardware Authentication Tokens (availability 3-6 months):	16
G/On 5 Software Authentication Token (Available today)	17
G/On 5 Hardware Authentication Token Overview.....	18
General Availability Release: G/On 5.3	19
Comparing G/On 5.3 with G/On 3.6	23
G/On 5 Road map and Statement of Direction	25
G/On 5.4 – Advanced Authentication and G/On 3.6 upgrade.....	25
G/On 5 Statement of direction	26
G/On 5.3 Hardware & Software Requirements.....	27
G/On 5.3 Documentation & Collateral	29
Training & Support	29
Technical Training	29
Giritech Support	29
G/On 5 License Model	30
Standard Feature Set of G/On 5.3.....	30
Optional Client Features.....	31
Optional Server Features.....	31
Menu Action Template Feature Requirement	33
G/On 5 Licensing, Pricing and Ordering	34
The G/On License File.....	34
How to obtain a G/On License File.....	35
License details overview	35
Pricing & End User License Agreement	36
Pricing	36
Upgrade Pricing.....	36
Ordering.....	36

Product Announcement Confidentiality: This document contains proprietary information, which is the confidential property of Giritech A/S and is restricted to Giritech Customers and Partners. Neither this document nor the information contained within are to be distributed, in whole or in part, by any means without prior authorization, including but not limited to printed, magnetic, electronic, or verbal forms.

G/On 5 Feature Overview

From a technical and networking perspective G/On 5 is a **client/server software solution implementing a distributed port forwarding proxy with built in application level firewall based on an application level communication protocol.**

Contrary to traditional VPN based solutions, G/On 5 does not connect remote devices directly to the company network. Instead, G/On 5 creates **secure virtual connections** between users and their applications, their office PC or a virtual desktop. Traditional VPNs create open tunnels between the remote PC and the company network and the security challenge is now to protect the tunnel from the unknown and unwanted. G/On takes the opposite and granular approach of creating individual connections between known users and known applications. And, these are the connections that G/On protects.

G/On 5 offers unique solutions to the challenges of providing secure access:

- Windows, Mac and Linux devices.
- Multi-factor user and device authentication based on state of the art industry strength smart card technologies.
- Mutual authentication to avoid Man-in-the-Middle (e.g. “phishing” and “pharming”) and “spoofing” attacks.
- Application connectivity enablement integrated with authorization policies and identity management.
- Unique virtualization and device isolation technology that keeps the device off the corporate network and reduces the attack surfaces for virus, trojans and spyware.
- Optional launch of G/On from the operating system on the remote device **or** using the **G/On Secure Desktop** option as a complete re-start of the remote device booting up a locked down secure Linux operating system with integrated G/On secure connectivity.
- Leading edge, FIPS 140-2 validated encryption technology for data protection and integrity.
- Integration with user directories for identity management, user group management, and user/group privilege management.
- Detailed XML formatted logging of *who, when, where, how, what* ready for reporting via standard report writers and a set of customizable standard reports.
- A client/server management suite of tools with role based user interface.

Building on more than four years of solid customer experience, the product announced today is a completely rewritten implementation of Giritech’s patented technology called EMCADS[®]

Background

Previously most of the professional IT infrastructures consisted of simple corporate PCs running Windows used to run local word processing and spreadsheet applications and connecting company employees to email and printers. In some cases combined with a few static point-to-point connections to key partners. Reporting was by spreadsheets designed for management and accountants once every quarter and security was primarily an issue of trying to prevent unauthorized people from entering your physical premises and the unauthorized copying of paper records.

All of this has changed dramatically in recent years – the number of computing platforms has exploded, companies' eco-system of users is increasingly complex and legal and financial tracking and reporting is more important than ever. Additionally, the number of applications to which different users need access has increased and as well security threats are increasing on a weekly basis. This ever-rising "tsunami" of business challenges makes the need for IT infrastructure simplification not just a *nice to have* but a fundamental *need to have*. The solutions designed for yesterday's challenges will no longer be able to support today's - not to mention tomorrow's business needs!

New user generations use computers all the time for communication, social networking, news updates, as TV and... work. Workers today don't just work in the office and they don't just do personal business at home. Already today, some businesses are realizing that it is not possible to force a new generation of employees to use a company PC that is locked down, managed and controlled by the company. Today, many people expect to be able to use their own device also for work. This is an impossible situation for corporate IT and requires a new paradigm where user devices never become part of the company network.

A different paradigm to corporate IT infrastructure is needed. A paradigm based on deep understanding of the real business needs and not on capabilities, or lack of capabilities, of technology. A paradigm designed around users and their day to day business. A vision of an end-to-end infrastructure connecting users to the applications they need. Giritech's solutions are built upon the paradigm of connecting users with applications while avoiding the challenges and threats from the network and the infrastructure. We call it *Secure Virtual Access*. *Secure* because security is a fundamental pre-requisite that has to be designed into all parts of a solution from the beginning. *Virtual Access* because we connect users with the applications and data without connecting the PC to the network where the applications are located.

G/On 5 represents the latest result of Giritech's efforts to implement the end-to-end paradigm of Secure Virtual Access. Compared to previous releases of G/On, the new generation of G/On broadens the use of G/On, sets a new standard for quality and lays the foundation for future Giritech innovation.

Innovating G/On: Version 5 Architecture and Technology

G/On 5 is an innovative new software platform based on international experience obtained from more than 700 G/On customers and their local Giritech partners. The new software platform has been developed using industry standard, leading edge software technologies to ensure a long-term solution platform for current and future needs and challenges.

The new G/On platform provides the foundation for future development via an open, plug-in based architecture allowing easy development of software to support new technologies. The G/On 5 architecture will enable Giritech to accommodate a wide range of customer and partner specific requirements.

The main characteristics of the new platform are:

- Scalable distributed client/server software architecture with separation of communication services and management services enabling a highly flexible implementation of G/On in existing or new infrastructures and ensuring cost effective support for installations ranging from a few users to tens or even hundreds of thousands of users.
- The use of cross platform software supporting a wide range of operating systems on client and server side.
- Targeted software technologies for specific areas of functionality, e.g. Eclipse as management GUI foundation, Python for business logic, C++ for communication core, web services, XML for open APIS and a range of other leading edge technologies.
- Support for leading edge and industry standard authentication technologies and customizable authentication policies.
- Abstraction layers between core G/On functionality and external services, such as SQL databases, operating system GUI's, license server, and identity management systems. These abstraction layers ease the integration with existing infrastructure and allow re-use of a wide range of existing tools and platforms already in place in most IT infrastructures.
- Plug-in architecture for future development of support for third party technologies via standardized and well-defined interfaces.

G/On 5 Solution Components

G/On 5 is designed to help users gain secure access to the applications they need while providing administrators full control over that access. Giritech has identified eight distinct functional areas to accomplish this task:



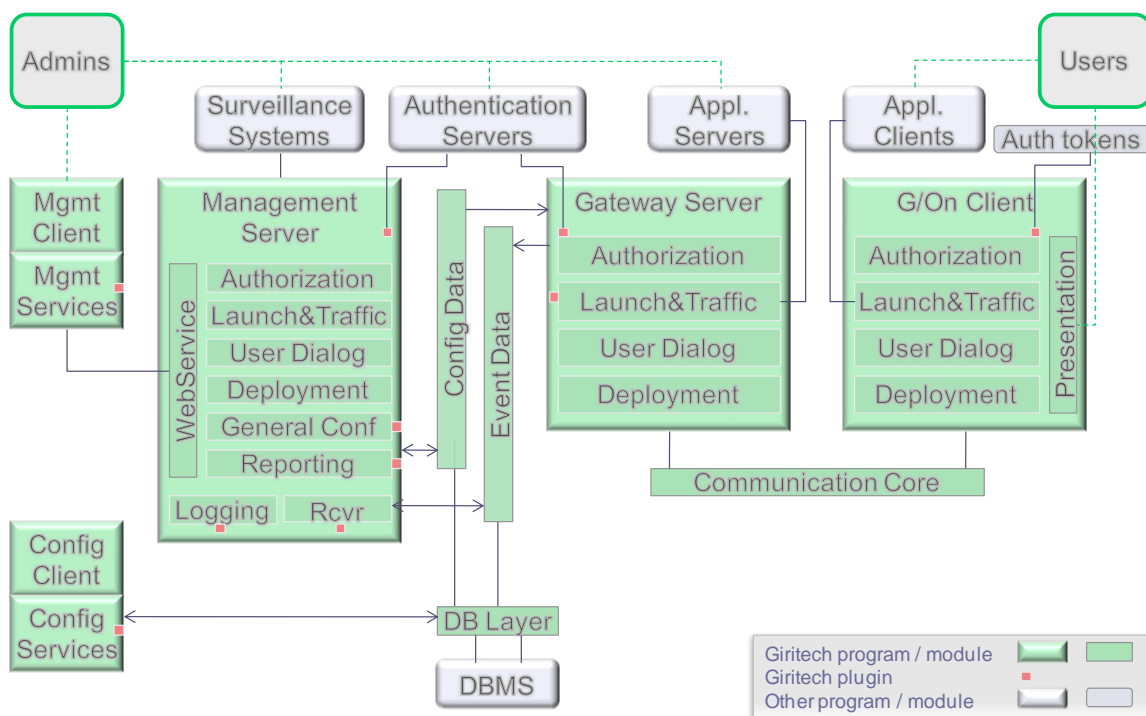
- Authentication, Authorization, Launch & Traffic and Communication constitutes the core

“G/On stack” where all the traffic between users and applications is controlled.

- The control functions of User Dialogue and Software Deployment provide users with a tailored, device adapted user experience and controls all necessary software required to enable and control access. The monitoring functions of Administration, Configuration and Reporting provide the G/On administrator with the tools required to implement, enforce and document the end-to-end *Access Policies*.

These eight areas of functionality are implemented in the client server architecture of G/On. However, all the functionality pertaining to enforcement of *policies and rules* is implemented on server side while the client side is focusing on user dialog and device isolation and independence. Consequently, the G/On server is the key component of G/On 5.

The component architecture of G/On 5 - or its software modules - is shown in the figure below. The functional areas just described above can be recognized below.



The main software components in G/On 5 are:

- The G/On Client
- The G/On Gateway Server
- The G/On Management Server

The Gateway Server and the Management Server together constitutes the **G/On Server**. Additional to these, a range of other components provide:

- User interface to the Management server (Mgmt Client)
- User interface for configuration (Config Client)
- Supporting services from non-G/On systems (Application interfaces, Authentication interfaces and Surveillance & Reporting system interfaces)

In addition to the core software system, G/On provides support for a range of authentication

tokens described in the following sections.

The overview illustration also indicates the primary application development interfaces (plug-in interfaces indicated by the red dots) where the architecture will be opened towards 3rd party components to support a wide range of future functionality.

The G/On Server

The G/On Server consist of one or more **G/On Gateway Servers** and the **G/On Management Server** and provides the core of all G/On functionality. It is the G/On Server that implements the functionality required for secure access from users to applications without the complexity of multiple firewalls, DMZ's, authentication, traffic inspection etc. as normally required by VPN based infrastructures. Thus, it is the G/On Server that provides the opportunity for achieving infrastructure simplification and cost savings of secure access.

Technically speaking the G/On Server *is a port forwarding proxy with built in application level firewall supporting an application level protocol* for communication with the G/On Clients.

From a traditional networking perspective the G/On Server implements:

- *Application level firewall.* The G/On Gateway Server and the **G/On Client** makes detailed inspection of all traffic and uses it to make decisions on what to allow and what to reject. This is similar to what can be done with other application level firewall solutions, but G/On is not just a standalone firewall as it controls the entire end-to-end communication and only allows traffic from authenticated users to authorized applications. G/On knows the user, knows the application client and knows the application server for each and every package transported and is using this information to make decisions on what to forward and what to reject.
- *Proxy functionality.* The G/On Gateway Server implements the G/On proxy functionality of separating *external* application *client* connections from the *internal* application *server* connections. The Gateway Server is key to the establishment of the *virtual* end-to-end connections essential to the G/On architecture.
- *Application Access Control (AAC).* As opposed to standard Network Admission Control (NAC), G/On provides no access to the network. Instead the G/On architecture is designed to enable detailed information about end-user devices to be collected and used as part of a complete authorization decision (device authentication). Only connections from authenticated users *and* from authenticated user devices can be authorized to access specific applications using specific application client software. Where classical NAC decides which devices are allowed access to the complete network (and what state these machines have to be in), the G/On AAC functionality instead focuses on the user and the application and using that information decides if the device the user happens to use is known by the G/On server or not. This is a simpler authorization decision, due to the understanding of what action the user is trying to perform instead of merely examining the device with no consideration of what the user does after being provided access.
- *Authentication of users.* Verifying remote users' identity via different multi-factor authentication solutions is a fundamental pre-requisite for meaningful security policies. The complexity arises when the company policies require different security levels and often require the use of different technologies to implement strong authentication. G/On

provides the foundation of consolidating a wide range of different authentication technologies and policies on one easily managed platform.

- *Security policy implementation and enforcement.* The **G/On Management Server** offers a *Single Point of Management* for implementing, documenting and enforcing access security policies. XML formatted logging of the traffic provides event alerts as well as reporting capabilities for internal and external auditing for compliance and regulatory purpose. The G/On server knows the user, the device, the connection, the application and the enforced authentication and authorization rules. Conveniently, G/On offers a central point of auditing capabilities and reporting.

A **G/On installation** consists of one or more *Gateway servers* and typically a single *Management server* depending on failover, load and administrative processes of the specific G/On customer thus avoiding “single point of failure” in G/On installations. For smaller installations, the Gateway servers and the Management server are typically installed and run on the same physical or virtual server.

The G/On Gateway Server allows or blocks individual connections between users and resources based on configurable authentication and authorization policies. The Gateway Server implements the server side of the connections between individual G/On Clients (forwarding traffic from application clients) and the application servers at the backend. The Gateway Server enforces all *decisions* regarding:

- *Authentication and Authorization:* the real-time communication with the authentication server, e.g. LDAP/AD, validation of tokens and devices and making the resulting authorization decision on what the user is allowed to access and how.
- *Launch & Traffic:* switching traffic and communicating with application servers, e.g. Terminal Servers, Exchange or Citrix farms. The Gateway Server decides what application client software to launch on the user device and instructs the G/On Client accordingly. When receiving traffic from the G/On Client on user devices the Gateway Server forwards the traffic to the specific application server.
- *User dialogue:* The G/On Client presents the results of authorization decisions to the end-user and responds to user actions about which applications to access. This functionality supports the existing end user experience of the client platform and generates the specific menus helping and guiding the user to the most relevant applications.
- *Deployment:* Distribution of the client software packages to G/On Client devices when requested by the user and/or the Management Server. The package based software deployment system provides configurable packages of software modules to be deployed to the client devices. The deployment features are used for the G/On client software but can be used for any software that needs to be deployed to client PCs.

All decisions are made by the G/On Gateway Server according to policies, rules and configurations established by the G/On administrator in the G/On Management Server (see below).

G/On’s **Single Point of Management (SPM)** is a client/server solution based on a G/On Management Server and a **G/On Management Client**. The G/On Management Server manages all configuration and setup of a G/On installation and is coupled to the G/On Gateway Server(s) to allow one management server to handle multiple Gateway servers. Consequently, G/On offers maximum flexibility for configuration of gateway servers, management server and management clients across multiple physical and virtual server environments. The G/On Management Client can connect through G/On itself to the G/On Management Server offering IT administrators secure remote access for G/On administration and reporting.

Furthermore, the G/On Management Server can be accessed via web services which enable the integration of the G/On management into existing administrative tools typically deployed in large IT operations. Giritech's own management client also uses that web services interface.

G/On Management provides different views, called "Perspectives" that implements the administration of a G/On system. The primary views are:

- Authorization Management
- Authentication Management
- Launch Management
- Token Software Management and
- Reporting

"Authorization Management", "Authentication Management" and "Launch Management" control user access to applications via the use of "Rules" (see below). "Token Software Management" controls software and updates on user devices and "Reporting" provides a GUI and tools to generate reports on usage and configuration.

"Rules" are simple statements that describe how a user (as identified by a username/password entry in a directory, e.g. user "demo" in Microsoft AD) is allowed to use a token (e.g. a G/On MicroSD) to get access to an application like "Mail" (for instance Windows Outlook). The rule can be described as:

```
<"demo@giritech.com" + "MicroSD 001" => "Windows Outlook">
```

This is to be read as: "User "demo" in domain "Giritech.com" (the AD) is given access to Windows Outlook **only** if he/she is able to present token "MicroSD 001" **and** provide the correct username/password to the AD.

This policy is enforced by the G/On Gateway Server and the G/On Management Client allows the G/On administrators to enter the rules into the system. All the policies of G/On are defined through similar rules that can be applied to individuals or groups to provide flexibility while minimizing the effort of creating the policies. Please consult the G/On documentation for purpose and syntax of all the rules.

Interpreting what "Windows Outlook" actually means in the above mentioned rule is tightly connected with the executables (the programs) allowed to run and what parameters the executables will be using. This is also configured in the G/On Server and forwarded to the G/On Client after authorization. The G/On administrator decides how to implement "Windows Outlook" under given circumstances. The administrator can for instance decide to implement the application "Windows Outlook" as an Internet Explorer browser directed to connect to the company's Outlook Web Access. Or it can be implemented as "Windows Outlook" by launching the locally installed Outlook.exe client software on the user device and telling it where to find the corresponding Exchange server. It can also be launched via other means like a Citrix desktop or a MS Terminal Server desktop. Which one of these (or other alternatives to use) is dependent upon company policies.

Executing these commands is done by the "Launch & Traffic" component which directs the G/On Client to launch specific software with specific parameters.

To help the administrator control what software *can be* executed and how it is configured, G/On provides a configurable software packaging system (the Software Deployment Tool) enabling the development of customized **G/On Client Software Packages** to be deployed to the user device. The packages are generated via templates, standard or customized, providing Giritech partners with opportunities to develop special configurations to address customer needs or to

design template-based standard solutions to be rolled out across a wide range of customer installations. A G/On Client Software Package is used by **G/On Menu Actions** which are the specific set of commands, associated parameters, and definitions that launches and runs the software on the user device and controlled by the G/On Client. The G/On Menu Actions are presented to the user in the G/On Menu based on authentication and authorization policies.

G/On Menu Actions are created by the G/On administrator via wizard-driven **G/On Menu Action Templates** that are specific to the application or type of application to be launched.

Consequently, a G/On Client Software Package is associated with one or more G/On Menu Action Templates that in turn are used to create one or more G/On Menu Actions for a particular Client Software Package. The xml-based Menu Action Templates can be customized and new templates can be defined allowing for the creation of complete sets of Client Software Packages and the associated Menu Action Templates.

G/On 5 comes standard with a set of Client Software Packages and associated Menu Action Templates:

Application	Menu Action Template					
	Windows client	Software Package	Mac client	Software Package	Linux client	Software Package
Remote Desktop access with Single Sign on	gtsc	Yes	rdc	Yes	rdesktop	In Linux
Access to My PC with Single Sign On	gtsc_my_pc	Yes	rdc_my_pc	Yes	rdesktop_my_pc	In Linux
Remote Desktop access	mstsc	In Windows				
Remote Desktop access to My PC	mstsc_to_my_pc	In Windows				
Access to Mac (Screen Sharing with single sign on)	tight_vnc	Yes	screen_sharing	Yes		
Access to My Mac (Screen Sharing with single sign on)	tight_vnc_my_pc	Yes	screen_sharing_my_pc	Yes		
Citrix Web Access with single sign on	citrix_web	Yes	citrix_web	Yes	citrix_web	From Citrix
Citrix Web Access for G/On Menu publication with single sign on	citrix	Yes	citrix	Yes	citrix	From Citrix
Browser	browser	In Windows	browser	In Mac OS	browser	In Linux
Internet Explorer	ie	In Windows				
Outlook Web Access	owa	In Windows	owa	In Mac OS	owa	In Linux
Outlook via http	outlook	Installed				
Generic Mail (POP3, IMAP)	generic_mail	Installed	generic_mail	Installed	generic_mail	Installed
Filezilla FTP down/upload	fz	Yes	fz	Yes	fz	In Linux
G/On Help Manager	gon_client_help_manager	Yes				
G/On Help Client	gon_client_help	Yes				
G/On Management	gon_management	Yes				
Secure Desktop					secure_desktop	Yes
Wake on LAN	generic_wake_on_lan		generic_wake_on_lan		generic_wake_on_lan	
Wake on LAN My PC	generic_wake_on_lan_my_pc		generic_wake_on_lan_my_pc		generic_wake_on_lan_my_pc	
Wake on LAN Generic	all_fields_wake_on_lan		all_fields_wake_on_lan		all_fields_wake_on_lan	
Citrix Generic	all_fields_citrix_web		all_fields_citrix_web		all_fields_citrix_web	
Generic single port applications	all_fields_single_port		all_fields_single_port		all_fields_single_port	

G/On Communication Core

The G/On **Communication Core** is the distributed software layer in the G/On stack connecting the G/On Clients and the Gateway Server(s). It is implemented in C++ to ensure maximum performance and easy portability to the range of client platforms (Windows, Mac and Linux) supported by G/On 5. The Communication Core is implementing the transport protocols of G/On and all transmission encryption (AES 256). It is based on a FIPS 140-2 validated encryption library ensuring compliance with the US governments guidelines for the use of encryption technology in the public and military sector.

The Communication Core is a separate software module in the G/On system enabling Giritech to upgrade to future encryption technology if/when needed.

The G/On Client

In addition to the authentication itself, all G/On token options are based upon the core G/On Client that handles the encrypted virtual connection to the G/On Gateway Server. Technically speaking, the G/On Client is a *port forwarding proxy* that captures data from an application client on a user's PC and forwards the traffic to the encrypted (and otherwise protected) connection to its corresponding G/On Gateway Server. The application client (e.g. local Outlook, a Remote Desktop (RDP) client or any other client of a client/server solution) effectively sees its corresponding application server as if it was co-located on the user PC. The connection created, controlled and protected by G/On is kept transparent to the communication between the application client and the application server.

The functionality of the G/On Client implements the client side support for:

- *Authentication and Authorization*: as controlled by the G/On Server and depending upon the supported list of authentication client options
- *Launch and Traffic*: launching the authorized application clients as outlined above and transporting the traffic between application client and network
- *User Dialog*: for login and presenting the result of the authorization to the end user controlling what and how the user is allowed to access applications
- *Deployment of local software* on the user device as requested by user or the G/On Server.

The G/On Client is thus an “extension” of the G/On Gateway Server implementing and enforcing the decisions made by the server. It is also the G/On Client that manages the actual user dialog and adapts the dialog to the device (e.g. OS) the user is running from.

The G/On user dialog component supports the user with activity indicators and different warning or notification screens, presenting the results of the final authorization decisions in the form of user specific menus and finally accepting and acting upon user selection of menu items. As with all client side functionality, configuration and setup of user dialog is controlled entirely by the G/On Server.

The G/On Secure Desktop

With the introduction of G/On 5, Giritech is also introducing an entirely new ground breaking technology, the **G/On Secure Desktop**. The G/On Secure Desktop is a feature that gives G/On users the option to boot the remote PC or Mac from their G/On USB Token and load a locked down Linux Operating System. In combination with new authentication tokens with CD-ROM and hardware encryption, it is possible to create a fully server managed G/On USB token with

known content and G/On Secure Desktop, thereby introducing a significant increase in the level of isolation between remote devices and the secure G/On connection. G/On Secure Desktop turns G/On into a very cost competitive, state-of-the-art security solution that meets most of the highest level security standards required by very security conscious organizations.

New G/On 5 Authentication Tokens

Giritech was first to market in 2004 with its innovative G/On USB that in one mobile device provides two-factor authentication and secure software storage for connectivity. The evolution of devices has since accelerated as CPU and memory circuits have reached new levels of integration with more and more functionality on smaller and smaller chips.

Giritech is therefore proud to offer the next state-of-the-art innovation within authentication tokens. The new G/On 5 solution is based on cryptographically secure **smart-card technology** thereby implementing a very strong **mutual** authentication protocol and completely avoiding the counterfeiting issue of copying devices.

Furthermore, as opposed to alternative smart-card based solutions, Giritech's solutions offer the user full device independence because the solution can be accessed and used on devices with limited login rights (no administrative rights required) **and** without requiring special drivers or other token specific software on the device. The new authentication tokens therefore combine leading edge technology and capabilities with the unique user convenience of G/On.

The advanced smart-card technology is provided by the highly visionary developer of new, integrated tokens, the German company, Giesecke & Devrient (G&D, www.gi-de.com). G&D is a leading developer of smart-card technologies for credit cards, access cards, and personal identification (PIV) cards. Giritech has worked closely with G&D to ensure that G&D's new generation of secure authentication, memory and encryption devices supports the functionality of G/On. Although G/On 5's plug-in architecture will enable the support of multiple different tokens, G/On 5 is developed specifically to support G&D's series of smart-card based tokens called *G&D StarSign® Mobility Token*.

At the time of general availability, G/On 5 supports two G&D tokens and it is the intent of Giritech and G&D to support all of the G&D StarSign Mobility Tokens within the next 3-9 months of this announcement.

G/On 5 Hardware Authentication Tokens available today:

G/On MicroSmart 1GB (based on *Giesecke & Devrient StarSign® Mobile Security Card*). This device is a standard microSD flash memory card combined with an additional integrated smart-card chip that is used by G/On for authentication. The flash memory is used for the storage of the G/On client software and associated application clients and data. The G/On microSD supports Windows, Mac, and Linux and can be used in mobile devices such as high speed broadband modems (e.g. USBConnect QUALCOMM 3G or HUAWEI Mobile Connect Modem E180 used by mobile carriers around the world), Laptops, PDAs and other mobile devices with a microSD interface. The G/On MicroSmart operates without any installation of drivers and doesn't require administrator rights on the device thus reducing costs for implementation, support and help desks.



G/On USB MicroSmart 1GB (based on *Giesecke & Devrient StarSign® Mobility Token μSD*). This G/On USB device offers a high degree of mobility, versatility and convenience as it supports Windows, Mac, and Linux based devices with a USB port. It uses the same integrated smart-card and microSD flash memory for storage as the G/On MicroSmart but is housed in an adapter specially built for the higher heat emission of this special microSD card. The G/On USB MicroSmart requires no installation of drivers and can be used on any PC and does not require administrative rights.



Planned G/On 5 Hardware Authentication Tokens (availability 3-6 months):

G/On USB SafeSmart 1GB (Based on *Giesecke & Devrient StarSign® Mobility Token Classic*). This USB device contains flash memory, a separate CD-ROM partition, a flash controller supporting data encryption, and a smart-card and supports Windows, Mac and Linux. Provided the ability of the operating systems, this device offers automatic launch of the G/On client without any prior installation or administrator rights. The G/On USB SafeSmart permits automatic encryption of data stored on the token fully transparent to the user and the smart-card ensures the security of the identities stored on the token. In one single device, the G/On USB SafeSmart offers protection of data in transit as well as at rest.

G/On USB MultiSmart 1GB (Based on *Giesecke & Devrient StarSign® Mobility Token ID1*). This device provides the ultimate secure access solution by combining G/On with existing smart-cards for Personal Identity Verification (PIV) and supports Windows, Mac and Linux. Chip cards in ID1 format can be inserted into the device and be used as G/On authentication. A second smart-card is included and can be used for authentication of the device in the case the PIV card issuer does not provide software access. The G/On USB MultiSmart functions as a user-friendly, driverless card reader in mini format and includes flash memory, hardware data encryption, CD-ROM partition, and an ARM7 processor. Except for drivers potentially required by the PIV card, the device itself requires no driver installation and does not require administrative rights on the PC.



G/On USB H3 1GB (Based on *Hagiwara UDRW G3 technology*). This **Windows Only** USB device contains flash memory, a separate CD-ROM partition, and a hidden memory zone accessible only to the G/On Server. The device offers automatic launch of the G/On Windows client without any prior installation or administrator rights, storage of G/On Client software on write protected CD partition and read/write memory for storage of data and application clients. Authentication functionality is based on a private key stored in a hidden memory zone. G/On USB H3 1GB was the standard token device used with earlier generations of G/On.

G/On Device Token This special token makes it **possible to use personal laptops or other personal computing devices as G/On authentication factors**. The G/On Device Token is created from a G/On SoftToken in combination with unique hardware information of the device including the MAC address of the network card(s). This option is particular valuable in these scenarios:

1. Businesses that are already providing personal laptops to employees and staff can

use these devices as the second authentication factor in addition to user name and password. The company saves the cost of separate authentication tokens and the logistics of managing these tokens. From a user perspective, the hardware part of the two-factor authentication becomes totally transparent.

2. Schools, colleges, and universities are more and more relying on students and staff using their own laptops for studies and work. The G/On Device Token enables the schools to allow students and staff to use these personal devices for secure access to campus network. Forcing two-factor authentication is critical in these environments for secure identification of user, the device and the resources that are accessed. The G/On administrator can from one centralized tool manage, control, and document who has access to what. G/On's Windows, Mac and Linux clients supports the most popular devices used in the educational sector today.

G/On 5 Software Authentication Token (Available today)

In addition to hardware based authentication tokens, G/On 5 also supports software based tokens. **G/On SoftToken** is a challenge-response based authentication using public key cryptography but without the need for a X.509 based Public Key Infrastructure (PKI). The soft-token is generated by the G/On Server and allows authentication of users from a wide range of hardware devices. *Note: Like other soft-token based solutions, the G/On SoftToken is not tied to the hardware device and should normally **only** be used on trusted hardware devices (computers, USB keys, external storage devices etc.).*

G/On 5 Hardware Authentication Token Overview

G/On 5 Hardware Authentication Tokens	MicroSmart	USB MicroSmart	USB SafeSmart	USB MultiSmart	USB H3
Availability	Now	Now	Dec 2009	Dec 2009	Dec 2009
Supported Operating Systems	Windows/Mac/Linux	Windows/Mac/Linux	Windows/Mac/Linux	Windows/Mac/Linux	Windows
Software Execution from Token	Yes	Yes	Yes	Yes	Yes
Zero Footprint	Yes	Yes	Yes	Yes	Yes
Driverless Operation – uses existing mass storage driver	Yes	Yes	Yes	Yes	Yes
Works for NON-admin users	Yes	Yes	Yes	Yes	Yes (No for CD update)
Authentication Method	Smart Card	Smart Card	Smart Card	Smart Card	Protected SoftToken
CD ROM partition for read only storage of G/On Client	No	No	Yes	Yes	Yes
Flash Memory	1GB	1GB	1GB less size of CD ROM	1GB less size of CD ROM	1GB less size of CD ROM
Hardware data encryption	No	No	Yes	Yes	No
Exchangeable Smart Card (SIM-format)	No	No	Yes	Yes	n/a
Built-In PIV ID1 Smart Card reader	No	No	No	Yes	n/a

General Availability Release: G/On 5.3

The first generally available release of G/On 5 is version 5.3. Previous releases of G/On 5 have been production releases 5.1 and 5.2 with limited functionality for specific customers.

This section describes the most important features and functions in G/On 5.3. More details can be found in the G/On 5 Manual and on the Giritech website.

Feature	Description
Autostart	<p>Autostart of G/On client software upon token insertion without requiring additional icon selection and activation by the end user.</p> <p>Benefits: Auto launches the G/On login process when inserting the token into the end user device. The user only inserts the G/On token into the PC and awaits the normal G/On login window. This feature, together with single sign-on (see later), will provide the simplest possible login process for end users.</p> <p>Related Known Issues: Mac OS X, Linux and Windows 7 do not support autostart from non CD-ROM partitions and consequently autostart is not supported on the G/On MicroSmart and G/On USB MicroSmart tokens.</p>
Citrix Single Sign On	<p>“Re-uses” the username/password used for G/On authentication to implement single sign-on to Citrix.</p> <p>Benefits: Allows reuse of G/On login credentials (validated against an AD or LDAP) as login to Citrix. The end user only enters login credentials (username/password) once and thus does not have to re-enter credentials when launching Citrix applications from the G/On menu.</p> <p>How to use: The G/On 5 Citrix single sign on is implemented server-side and does not forward or expose in any way user credentials client side. No user involvement is required, all setup and administration is done server-side controlled by the G/On administrator. Works with Citrix Web Client on Windows, Mac and Linux.</p>
Terminal Services Single Sign On	<p>“Re-uses” the username/password used for G/On authentication to implement single sign-on to Terminal Services.</p> <p>Benefits: Allows reuse of G/On login credentials (validated against an AD or LDAP) as login to applications. The end user only enters login credentials (username/password) once and thus does not have to re-enter credentials when launching applications requiring additional logins from the G/On menu.</p> <p>How to use: No user involvement is required, all setup and administration is done server-side controlled by the G/On administrator. Works with Terminal Services RDP client on Windows, Mac and Linux.</p>
“No Install” G/On client software	<p>The G/On client side software requires no installation and additional software, drivers or registry entries to function. Makes G/On run from virtually any PC with Internet access running a G/On supported operating system.</p> <p>Benefits: Allows IT administrators to control the client side software used when logging into the G/On server without relying on any local software on the end user device. Ensures the end user that login does not require downloads and/or installs of any software on the end user device before login. Does not require admin rights and helps ensure no traces are left on the remote PC.</p> <p>How to use: Natively supported by the G/On client software. Does not require special setup or administration.</p> <p>Related Known Issues: None.</p>
“No Install”	The G/On client can launch application clients directly from the G/On Token devices

application clients	<p>provided they do not require installation on the remote PC. These types of application clients do not require installation, drivers or registry entries to function and enables G/On to launch application clients to connect securely to the corresponding application server. Included with G/On comes Remote Desktop Client and Citrix Web Client.</p> <p>Benefits: Allows IT administrators to control the client side application software used when launched by G/On.</p> <p>How to use: Natively supported by the G/On client software. Does not require special setup or administration.</p> <p>Related Known Issues: Some application clients do require installation on the remote PC. These applications must either be installed already or must be installed prior to being launched by G/On. Many application clients may be “virtualized” by tools such as Thin4App from VMWare that allows installed applications to be packaged and run from a USB device. Distribution of such solutions to devices can be managed by the G/On Server.</p>
Customizable Authentication policies	<p>Customizable Authentication policies allow the G/On administrators to define the meaning of an “authenticated user” in compliance with company policies. Different users or groups of users may be required to have different authentication policies depending on their role, what they need access to and their association with the company.</p> <p>Benefits: The role based G/On Management Client provides a view for authentication rules where the G/On administrator in few steps defines how users or groups of users are authenticated.</p>
Customizable Authorization policies	<p>Customizable authorization policies allow the G/On administrator to define the applications users or user groups have access to once they are authenticated.</p> <p>Benefits: The role based G/On Management Client provides a view for authorization rules where the G/On administrators in few steps defines the specific applications or sets of applications users or groups have access to.</p>
Remote administration	<p>Remote management through G/On enables G/On administrators to work from any G/On connected PC with the G/On Management Client.</p> <p>Benefits: The G/On Management tool is a client/server application which gives maximum flexibility on how to configure the administrative tasks of G/On.</p>
Customizable software deployment system	<p>Customizable client software package management enables the distribution and maintenance of remote software on end user devices. Primarily targeted at maintaining G/On and associated 3rd party application client software, but will support almost any local software and/or data on the end user device if needed.</p> <p>Benefits: This feature ensures that all administration of software on end user devices is administrated and maintained from the central G/On server under the full control of the G/On administrator. Besides the control and security benefits, this feature also simplifies software maintenance and distribution and eases the user experience of downloading additional software or new versions to end user devices. When a user is authorized to use an application client for which the necessary local software is not available, the software deployment system will enable and guide the user to download and install the missing components on an “as-needed” basis.</p>
Open Reporting interface	<p>The G/On server collects detailed information on end user access and behavior that can form the basis for reports satisfying a range of compliance needs. Giritech delivers a set of default reports and an associated report viewer (BIRT – Business Intelligence and Reporting Tool - viewer and repository, see: http://www.eclipse.org/birt/phoenix/) as part of the standard G/On package, but the reporting web-interfaces are open to other reporting tools already being deployed in the customer’s organization.</p> <p>Benefits: Provides a detailed basis for the development of customer specific reports about system usage and end user behavior. By providing an open interface (XML based) it becomes a simple exercise to integrate with existing solutions in customer installations. At the same time the standard BIRT based solution delivered with G/On 5 provides a basic set of reports to enable customers <i>without</i> an existing reporting solution to begin rolling out more effective compliance reporting.</p>

AES 256 bit encryption	<p>FIPS 140-2 validated AES 256 bit encryption is the basis for all transmission of data between G/On clients and runtime server. The NSA approved AES 256 remains one of the strongest mainstream encryption algorithms available for protecting data “in transit”.</p> <p>Benefits: By using a state of the art approved strong encryption algorithm, such as AES 256, G/On administrators can rest assured that eaves dropping and other attacks on G/On protected traffic in transit between clients and servers will not be successful.</p> <p>How to use: Embedded in G/On. No special configurations required, all traffic transported between G/On clients and G/On runtime server will be protected by AES 256 encryption.</p>
Lock-to-Process	<p>“Lock-to-Process” is a Giritech technology that controls which application software client is allowed to use an established G/On connection. The technology “locks” the two processes (the application client and the G/On client) to each other by ensuring that only specific processes with well known processID’s launched by the G/On client is allowed to use the G/On connection.</p> <p>Benefits: Part of Giritech’s end user device independence strategy.</p> <p>How to use: To be enabled – or disabled - via the G/On Management. Security policies decides if “Lock-to-Process” is to be enforced or not on the end user device.</p>
Application Access	<p>Contrary to normal VPN technology G/On does not connect the remote device to the company network. G/On connects known users with known applications, the users’ office PC or a virtual desktop.</p> <p>Benefits: G/On provides access to exactly the specific applications to which the individual user has been authorized. G/On provides true end-to-end connectivity which is a fundamental pre-requisite for providing full enforcement of the security policies described by the company.</p> <p>How to use: Integral part of G/On Management.</p>
Advanced Authentication Tokens	<p>G/On 5.3 supports the two new devices:</p> <ul style="list-style-type: none"> - G/On MicroSmart 1GB - G/On USB MicroSmart 1GB <p>Related known issue: G/On 5.3 does NOT support the existing G/On USB G1, G2, and G3 from Hagiwara. Support for existing G/On USB G2 and G3 keys is planned for the release of G/On 5.4.</p> <p>Notice: There is no plan to support the original G/On USB G1 (64MB).</p>
Advanced Authentication Tokens: G/On soft-token	<p>The G/On Soft-token is a software generated public-private key pair. The G/On administrator creates the G/On Soft-tokens directly in G/On Management and consequently requires no additional external PKI. The G/On Soft-token is a public-private key pair, with the private key saved in a separate file (the token) to be used by the G/On Client to connect to the G/On Server. The server is able to validate the key using the public key saved on the G/On Server.</p> <p>Benefits: Because the G/On Soft-token is based on a small file it is easily distributed to PC’s or external memory devices thus allowing access from a wider range of devices. This solution requires the user to ensure the physical and virtual security of the device and it is recommended only to use G/On Soft-tokens on trusted devices!</p>
Client side Operating System support	<p>Client side operating systems and platforms supported include:</p> <ul style="list-style-type: none"> • Windows XP (32 bit) • Windows Vista • Windows 7 • Apple Mac OS X 10.4 (Tiger) • Apple Mac OS X 10.5 (Leopard) • Apple Mac OS X 10.6 (Snow Leopard) • Linux Fedora 11 with GTK+ GUI (32 bit) <p>Benefits: Supporting a wide range of client side operating systems enables IT administrators to implement access from a very wide range of user devices, including company owned and managed to personal unmanaged devices. The different G/On clients supporting the different operating systems also provides a native operating system specific user interface, adapted to the capabilities and “look & feel” of the different operating systems.</p>

	<p>Related Known Issues: Windows 2000 and XP (64 bit) may work but are not fully tested G/On 5 client platforms.</p>
Server side Operating System support	<p>Overview: server side operating systems and platforms supported include:</p> <ul style="list-style-type: none"> • Windows Server 2003 R2 • Windows Server 2008 <p>Benefits: Windows Server 2003 is the most widely used server operating system in the world with Server 2008 positioned as the upgrade path from Windows Server 2003. Support for these server operating systems ensures straightforward interoperability with existing support process and infrastructure.</p>
Database Systems support	<p>DBMS platforms supported include: Built-in (sqlite) SQL Server 2005 (in a limited Giritech recommended setup for G/On 5.3)</p>
User Directory support	<p>User Directories supported:</p> <ul style="list-style-type: none"> • Microsoft Active Directory (AD) • Standard LDAP (e.g. Novell eDir)
HTTP Encapsulation	<p>The Giritech HTTP Encapsulation option enables G/On traffic to traverse HTTP proxies by encapsulating G/On TCP traffic as HTTP traffic.</p> <p>Benefits: The HTTP Encapsulation option tool increases the ability of the G/On Client to connect to the Internet from local networks that only allow outgoing traffic through HTTP proxies. This feature complements the existing support for multiple outgoing ports.</p> <p>Related Known Issues: Has been tested with Microsoft's ISA server, Jana server 2 and Squid. As proxies are very different you might experience issues with other proxy installations or other related network elements, such as packet-inspecting firewalls and similar.</p>
Remote change of password in AD configurations	<p>Allows remote users to change login passwords via their G/On connection.</p> <p>Benefits: Removes the need for remote users to connect directly to the LAN in the office when changing user credentials.</p>
Integrated Wake on LAN (WOL) support	<p>Wake on Lan (WOL) is used to turn on computers on the LAN from remote locations.</p> <p>Benefits: Enables administrators to provide remote access to existing desktop PC's without the costs of having the PC's running at all times.</p> <p>Related Known Issues: Wake On LAN technology must be supported and enabled on the PCs that is expected to react on the WOL request. WOL uses broadcast addresses on the LAN. These addresses must be forwarded by local routers on the LAN. Sometime this type of traffic is filtered out to avoid overloading the LAN.</p>
Dynamic user menus	<p>The individual user menus generated as a result of the authorization process are dynamically and automatically created after each authorization decision. The menus will therefore always reflect the allocated rights to each user under the given circumstances.</p> <p>Benefits: Enforces policies by only allowing users access to the applications they are authorized to use at any given time.</p>
Automatic "Top 3" user menu	<p>The dynamic user menu contains an automatic "Top 3" of the most used applications presented to the user. This facility eases navigation for the end user and provides an almost immediate access to the most important applications for the end user.</p> <p>Benefits: Simplifies end user experience.</p>

Comparing G/On 5.3 with G/On 3.6

This section provides a brief summary of the main differences between G/On 3.6, based on the previous technology platform and G/On 5.3 based on the new G/On 5 platform.

G/On 5 is an entirely new, significantly more powerful generation of Giritech's technology supporting Windows, Mac, and Linux clients, new authentication devices and methods, improved performance, and a new and more robust user interface for administration and management. However, the basic functionality and objectives of G/On 5.3 are the same as for G/On 3.6.

There are currently features in G/On 3.6 that are not yet available in G/On 5. This section also provides the G/On 5 road map to help you understand when new features are expected. Feel free to contact Giritech (support@giritech.com) if you have questions to the road map.

Legend:

Y: Yes, supported in G/On 3.6, G/On 5.3 or future G/On 5 releases respectively

L: Limited support, typically involving manual setup and administration

P: Planned

- : Not supported

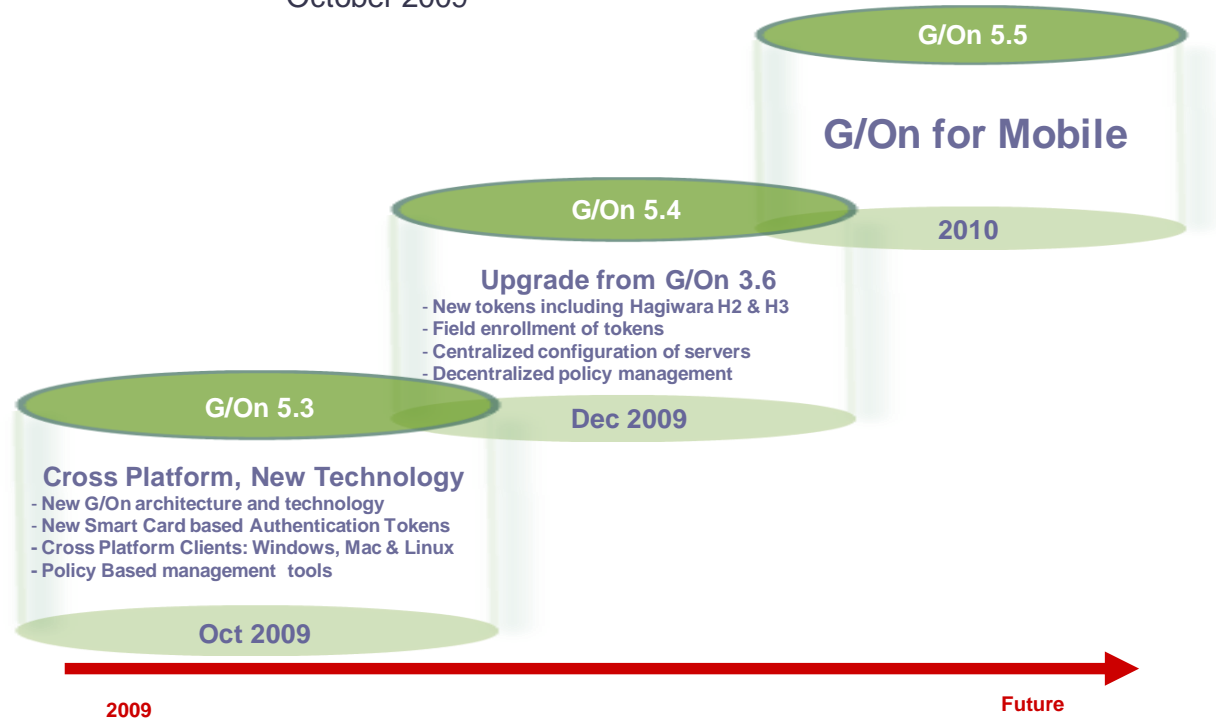
Feature	G/On 3.6	G/On 5.3	G/On Road map
Architecture:			
Distributed	-	Y	Y
Plug-in based	-	Y	Y
Separate gateway servers and management server	-	Y	Y
Client operating system:			
Windows 2000	L	-	-
Windows XP (32-bit)	Y	Y	Y
Windows Vista	Y	Y	Y
Windows 7	Y	Y	Y
Mac OS X 10.4 Tiger	-	Y	Y
Mac OS X 10.5 Leopard	-	Y	Y
Mac OS X 10.6 Snow Leopard	-	Y	Y
Linux Fedora 11	-	Y	Y
Future Fedora releases	-	-	P
Other Linux distributions (e.g. Ubuntu)	-	-	P
Mobile operating systems (Win Mobile, Android, iPhone OS, etc.)	-	-	P
Server operating system:			
Windows Server 2003 R2	Y	Y	Y
Windows Server 2008 SP2	Y	Y	Y
Linux (Red Hat)	-	-	Y
Support for Virtual Server installations	L	Y	Y
Database options:			
Built-in	Y	Y	Y
External SQL 2005	Y	L	Y
External SQL 2008	Y	-	Y
Server features:			
Duplicated Servers	Y	L	Y
Built-in load balancing	-	L	Y
Client features:			
HTTP Encapsulation (HTTP Proxy support)	Y	Y	Y
Connection Failover	Y	Y	Y
"No installation" client software	Y	Y	Y
"Minimal footprint" client software	Y	Y	Y
Authentication technology:			
AD validated username/password	Y	Y	Y
Change AD password	Y	Y	Y
LDAP validated username/password	3 rd Party	Y	Y
Hardware token - Hagiwara G1	Y	-	-
Hardware token - Hagiwara G2, G3	Y	-	Y
Hardware token – G&D StarSign Mobile Security Card	-	Y	Y
Hardware token - G&D StarSign Mobility Token μSD	-	Y	Y

Hardware token - G&D StarSign Mobility Token Classic	-	-	Y
Hardware token - G&D StarSign Mobility Token ID1	-	-	Y
Soft-token	-	Y	Y
Hardware token - Computing Device (G/On Desktop)	Y	-	Y
Other security features:			
Customizable Authentication policies	-	Y	Y
Customizable Authorization policies	Y	Y	Y
FIPS 140-2 validated AES-256 encryption	Y	Y	Y
Protected encryption key (for support of TrueCrypt or similar)	Y	-	Y
Support for hardware based USB encryption	-	-	Y
"Lock-to-Process" support	Y	Y	Y
Virtual Application Access (not VPN)	Y	Y	Y
Protocol support:			
IPv4	Y	Y	Y
Ipv6	-	-	Y
TCP	Y	Y	Y
UDP	Y	-	Y
SOCKS	Y	Y	Y
FTP (via 3 rd party software)	Y	Y	Y
End-user experience:			
Dynamic user menus	Y	Y	Y
Device dependent menus (called "Zones" in 3.x)	Y	-	P
Flexible customized splash screens	Y	Y	Y
Single Sign-On (Citrix, TS)	Y	Y	Y
Auto-run (where possible)	Y	-	Y
Simplified "Top 3" menu	-	Y	Y
Native operating system GUI	Y(only Windows)	Y	Y
On-Screen Keyboard	Y	-	Y
Login "brute force" protection features	Y	-	Y
Single Sign-On support:			
GTSC (password forward for RDP)	Y	Y	-
GICA (password forward for ICA)	Y	-	-
Citrix Web Interface (ICA proxy) with single sign on	-	Y	Y
RDP proxy	-	-	Y
VMWare View	L	L	Y
Other protocol specific proxies	-	-	P
Administrator experience:			
New, improved look & feel	-	Y	Y
Server setup wizard	-	Y	Y
Upgrade wizard	Y	L	Y
Policy based administrator GUI	-	Y	Y
Client/Server based management tool for secure remote administration	-	Y	Y
Semi-automatic enrollment of tokens	Y	-	-
Mass deployment of tokens	Y	-	Y
Integrated end user support (G/On Help)	Y	Y	Y
Reporting:			
Advanced Log-files	Y	Y	Y
Extensible Reporting (BIRT support)	-	Y	Y
Basic set of Reports	-	Y	Y
Advanced set of standard Reports	-	-	Y
Remote Software management:			
Managed Server-side (centralized mgmt of remote software)	Y	Y	Y
Automatic push of client software	Y	-	Y
On-demand download of client software	-	L	Y
Simple directory based	Y	-	-
Advanced package based	-	Y	Y
Customizable package management	-	Y	Y
Licensing:			
Basic licensing support	-	Y	Y
Online license acquisition	Y	-	Y
Offline license acquisition	Y	Y	Y

G/On 5 Road map and Statement of Direction

Giritech G/On 5 road map

October 2009



Future releases of G/On 5 will continue to add features increasing the value and versatility of G/On in an increasing range of company infrastructures.

G/On 5.4 – Advanced Authentication and G/On 3.6 upgrade

The primary focus for the planned G/On 5.4 release is the support for upgrade of G/On 3 installations (including the support for G/On USB H2 and H3 keys) and the addition of more authentication token options.

In summary, the current plans for G/On 5.4 include:

- A semi-automatic upgrade path from G/On 3 based installations requiring some manual setup (G/On 3.5 and G/On 3.6 – older versions of G/On 3 will have to be upgraded to G/On 3.6)
- Support for G/On 3 USB tokens (supports Windows only!):
 - o G/On USB H3 1GB (announced with G/On 3.5 in November of 2008)
 - o G/On USB H2 128MB, 512MB and 1GB (announced with G/On 3.3 in May 2007)
 - o **Please note:**
 - The G/On USB H2 and H3 can **ONLY** be used for Windows.
 - The G/On USB H2, 128MB will **only** support G/On 5 in a minimum configuration including the G/On 5 Client software and the G/On RDP client (GTSC.exe).
 - There is **NO** support for G/On USB H1 tokens (phased out with G/On 3.3 in May 2007)

- Please contact Giritech for a special offer on exchanging H1 with the new G/On 5 tokens or G/On USB H3 1GB (for Windows only).
- Support for more of the new advanced authentication tokens:
 - G/On USB SafeSmart 1GB
 - G/On USB MultiSmart 1GB
- Plus a wide range of additional administration and user experience features

G/On 5 Statement of direction

The continued increase in the versatility of G/On 5 builds upon the flexibility of the underlying technology platform by the use of the API's in the G/On 5 platform.

The most important directions for the future development are concerned with adding options to enable G/On administrators define and enforce a wider range of different access policies. This means adding more authentication options, support for a wider range of applications and supporting more operating system platforms and devices, especially on the client side. Furthermore, G/On closely follows the evolution of server side infrastructures (e.g. Virtualization, IPv6 etc.) in order to continue to ease the integration of G/On with existing and future IT infrastructures.

There are currently four main areas of development for G/On 5:

- More Authentication options
- Support for more operating systems
- Support for more client devices
- Support for more advanced enterprise backend infrastructures

Each of these areas is detailed in the following with a brief list of the currently expected features to be added to near-future releases of G/On in the 2010 timeframe.

More authentication solutions:

- SMS distributed passwords
- One Time Passwords
- Yubikey (www.yubikey.com)

Additional client operating system support:

- More Linux (Ubuntu)
- Google Chrome

Mobile client support (*the current focus for G/On 5.5*):

- Windows Mobile 6.1
- iPhone OS 3
- Android 1.5
- Symbian

Enterprise strength:

- Failover
- Redundancy
- Improved rollout process
- Linux server side operating system support
- Decentralized policy management
- Centralized server configuration and surveillance

G/On 5.3 Hardware & Software Requirements

The G/On Server requires the following:

- Hardware requirements: Minimum available hard disk space: 200MB
Minimum 1.2GHz Processor
Minimum 512MB memory for up to 100 concurrent users
Minimum 2GB memory for a maximum of 500 concurrent users
- Software requirements: Microsoft Windows Server 2003 R2 SP2
Microsoft Windows Server 2008 SP2
**Both 32 and 64 bit versions are supported*
- Firewall requirements: Port 443 set for "Through Traffic" (Default)
**G/On can be configured for other ports, e.g. 3945 or 80.*

The G/On Client requires the following:

- Minimum Storage: 128MB in a minimum configuration for the Windows client, Remote Desktop access (RDP), Citrix Web Interface, FileZilla.

Recommended Minimum Storage is 1GB to run Windows, Mac, and Linux clients and a typical set of application clients such as RDP, Citrix, Filezilla, and the G/On Management Client.

G/On Secure Desktop: Recommended Minimum Storage is 1GB to run Windows, Mac, Linux and G/On Secure Desktop along with RDP, Citrix and FileZilla.

G/On MicroSmart 1GB token requires the following:

- Hardware requirements: Micro SD port/adaptor
Minimum one virtual drive mapping available (e.g. drive E:\)
- Software requirements: Latest version of one of the following:
Microsoft Windows XP
Microsoft Windows Vista (32/64 bit)
Microsoft Windows 7 (32/64 bit)
Apple Mac OS X 10.4 (Tiger)
Apple Mac OS X 10.5 (Leopard)
Apple Mac OS X 10.6 (Snow Leopard)
Linux Fedora 11

G/On USB MicroSmart 1GB token requires the following:

- Hardware requirements: USB port version 1.1 and higher
Minimum one virtual drive mapping available (e.g. drive E:\)
- Software requirements: Latest versions of:
Microsoft Windows XP
Microsoft Windows Vista (32/64 bit)
Microsoft Windows 7 (32/64 bit)
Apple Mac OS X 10.4 (Tiger)
Apple Mac OS X 10.5 (Leopard)
Apple Mac OS X 10.6 (Snow Leopard)
Linux Fedora 11

Tested Application Clients:

G/On has been tested with the following application clients:

Latest version of Citrix®

Latest version of Microsoft® Windows® Terminal Server

- **Note:** G/On does not support the following TS 2008 features:
 - TS 2008 Remote apps
 - TS 2008 Gateway
 - TS 2008 Web Access

Browser:

If an application uses Microsoft® Active Server Pages®, Microsoft Internet Explorer is required. If application is Java-based, no specific browser is required. Please note that Microsoft® Internet Explorer does not provide out-of-the-box Java support.

G/On 5.3 Documentation & Collateral

Technical documents such as the G/On Manuals and various White Papers, as well as sales and marketing collateral are available via the Giritech website at <http://www.giritech.com/>

Training & Support

Technical Training

Giritech offers two day technical training classes covering an overall introduction, installation, configuration, and enablement of a number of client/server solutions including Citrix, Remote Desktop, Outlook, FTP, Browsers, etc.

Two day training class are currently scheduled for

Tuesday + Wednesday, November 4+5, 9:30 – 16:00

Tuesday + Wednesday, November 11+12, 9:30 – 16:00

Tuesday + Wednesday, November 25+26, 9:30 – 16:00

at the company address:

Giritech A/S
Spotorno Alle 12, 2.sal
DK-2630 Taastrup
Denmark

Please register for training by email to slb@giritech.com.

The cost for training is EURO 700 (DKK 5.000, USD 1.000) per person. Cancellations are accepted until 24 hours before scheduled training start. Late cancellations will be charged 50% of the training cost.

Giritech Support

Giritech offers support on G/On 5 to our partners in Denmark, North America and in the UK. Other markets are supported by local Giritech offices. Please consult www.giritech.com/int/Contact/Country-Offices for details.

Our partners can request support online via support@giritech.com, via our website at www.giritech.com or in urgent cases via telephone on +45 70 277 282.

Support is available during normal office hours (9:00 – 16:00 CET = 03:00am – 10:00am EST).

G/On customers can obtain support directly from Giritech through the purchase of a Service and Support agreement. Please contact Giritech for details.

G/On 5 License Model

The license model for G/On 5 is based on a Server License comprised of four different components: User Access License, Token Access License, Server Features and Client Features.

1. User Access License

The G/On Server must be licensed for all the users that it will be managing. A user is identified by a User ID and each User ID requires a User Access License (UAL).

2. Token Access License

The G/On Server must also be licensed for all the Authentication Tokens that it will be managing. Each G/On Token that is enrolled for access to the G/On Server requires a corresponding Token Access License (TAL).

- a. Additional TALs are required for users having more than one G/On Authentication Token such as a G/On USB and a laptop with the G/On client installed and using G/On Soft-token for authentication.
- b. Additional TALs are also required if the more than two factors for authentication is required. For instance, (however, not currently available) in addition to the G/On USB token, a RSA Token, a finger print reader or a SMS one time password may be required.

3. Server Feature

The G/On Server comes with a standard set of features and a set of optional features that can be licensed individually. Some of the optional features are licensed in quantities.

4. Client Features

In addition to the G/On Client itself, certain client features can be licensed for all or a subset of G/On Clients. Client Features are licensed by the number of G/On Tokens or devices they are installed on.

Standard Feature Set of G/On 5.3

The standard feature set of G/On 5.3 provides the following functionality:

1. G/On Client for Windows, Mac and Linux client operating systems
2. Two-factor Authentication
 - Notice:** *External user directory required for user authentication!* Either
 - a. Microsoft Active Directory and corresponding G/On Server Feature Active Directory User Directory, or
 - b. LDAP compliant user directory and corresponding G/On Server Feature LDAP User Directory
3. Support for single user directory/single domain
4. FIPS 140-2 validated, 256bit AES encrypted remote communication
5. G/On Client connection on one IP address or DNS name and on one IP Port
6. Up to twenty menu actions for enabling of **single port TCP based client/server applications** including (but not limited to):
 - a. Windows Remote Desktop access to Windows server/desktop with single sign on
 - b. Windows VNC Remote access to Mac

- c. Linux Remote Desktop access to Windows server/desktop with single sign on
 - d. Mac Screen Sharing for remote access from Mac to Mac with single sign on
 - e. Browser and browser based applications including Outlook Web Access (OWA)
 - f. Outlook over HTTP
7. Dynamic user menus with “autolaunch” capabilities
 8. User requested update of G/On Client software and client software packages
 9. Includes support for the following authentication tokens:
 - a. G/On MicroSmart 1GB
 - b. G/On USB MicroSmart 1GB
 - c. G/On SoftToken
 10. Logging and reporting

Optional Client Features

G/On Secure Desktop	This feature enables the bootable secure Linux operating system from a G/On USB Token. The feature is licensed for the total quantity of G/On Tokens that it must be enabled for.
G/On Help Client Standard	This feature enables the G/On Help Client Standard from a G/On Token or device. The feature is licensed for the total quantity of G/On Tokens and devices that is must be enabled for.
G/On Help Client Advanced	This feature enables the G/On Help Client Advanced from a G/On Token or device. The feature is licensed for the total quantity of G/On Tokens and devices that is must be enabled for.

Optional Server Features

Additional Gateway Servers	A G/On 5 license comes default with one G/On Gateway Server. Additional Gateway Servers for fail-over and load balancing can be acquired. All Gateway Servers must be managed by one and the same G/On Management Server. This feature requires MS SQL Database connectivity and it typically requires Multiple Client Connect IP Addresses unless the gateway server cluster is connected via a load balancer.
Multiple Client Connect IP Addresses	By default, G/On offers a single IP Address for the G/On Client to connect to. This feature allows the configuration of multiple IP Addresses to be defined for G/On Client to connect to for fail over purposes or load balancing. This feature is typically required when there is more than one Gateway Server.
Multiple Client Connect IP Ports	By default, G/On offers a single IP Port for the G/On Client to connect to. This feature allows the configuration of multiple IP Ports to be defined for G/On Client to connect for alternate ways to reach the Internet from a local network.
HTTP Encapsulation	This option allows the configuration of HTTP Encapsulation for the G/On Client to reach the Internet from a local network via HTTP proxies.
Multiple AD Domains NOT AVAILABLE IN G/On 5.3	By default, G/On allows authentication of users in a single Microsoft AD domain. This option allows authentication against multiple AD domains. PLEASE BE AWARE THAT LIMITED MULTIPLE DOMAIN FUNCTIONAL-

	ITY IN 5.3 IS SUPPORTED ONLY VIA MANUAL CONFIGURATION.
LDAP User Directory	This option allows authentication of users against any LDAP compliant user directory. Notice: G/On 5.3 requires an external user directory for user information and authentication. Consequently, either this feature or MS Active Directory User Directory is a required feature.
MS Active Directory User Directory	This option allows authentication of users against Microsoft Active Directory. Notice: G/On 5.3 requires an external user directory for user information and authentication. Consequently, either this feature or LDAP User Directory is a required feature.
MS SQL Server Database	By default G/On 5 uses an internal sqlite based database for storing G/On 5 data. This optional feature enables support for the MS SQL Server. This feature is required for running multiple gateway servers for shared cluster information.
Additional 10 Menu Items	By default, G/On 5 will offer 20 menu items. This feature will enable 10 additional menu items.
Login Notification Mail	G/On 5 offers the optional feature to send an email to users for verification of their login.
Welcome Message	G/On 5 offers the optional feature to issue a message to user after authentication but before the display of menu. Can be used to obtain user acceptance of access terms and conditions.
Multiport Port Forward	G/On 5 offers the optional feature to enable applications that communicate via multiple IP addresses and ports and consequently requires a more advanced port forwarding mechanism. This feature is required for running Outlook via fixed port configuration.
Launch Parameter File	G/On 5 offers the optional feature to dynamically create parameter files (such as .ini files) to be passed on to applications in a G/On menu action. Provides additional application launch capabilities. This feature is required to run Mac RDC, Filezilla and Windows MSTSC (not required for Giritech's GTSC).
Wake On LAN	G/On 5 offers the optional feature to issue commands to start PCs in stand-by mode or hibernated. The function of this feature depends on properly configured infrastructure.
Citrix Web Interface	G/On 5 offers the optional feature of integrated Citrix Web Access with server side single sign on. This feature includes the ability to publish the individual Citrix applications directly in the G/On Menu providing users with a convenient and seamless, single sign on interface. This feature is required to run any Citrix Web Access applications.

Menu Action Template Feature Requirement

G/On 5.3 includes a number of Menu Action Templates that helps the G/On administrator to build the G/On Menu Actions needed to enable applications for users. Some of these menu actions require a license to certain server and client features. The table below gives an overview of the corresponding Menu Action Template and G/On Server & Client features required to use them.

Menu Action Template Feature Requirement						
Application	Menu Action Template Windows client	Feature Required	Menu Action Template Mac client	Feature Required	Menu Action Template Linux client	Feature Required
Remote Desktop access with Single Sign on	gtsc		rdc	Launch Parameter File	rdesktop	
Access to My PC with Single Sign On	gtsc_my_pc		rdc_my_pc	Launch Parameter File	rdesktop_my_pc	
Remote Desktop access	mstsc	Launch Parameter File				
Remote Desktop access to My PC	mstsc_to_my_pc	Launch Parameter File				
Access to Mac (Screen Sharing includes single sign on)	tight_vnc		screen_sharing			
Access to My Mac (Screen Sharing includes single sign on)	tight_vnc_my_pc		screen_sharing_my_pc			
Citrix Web Interface with single sign on	citrix_web	Citrix Web Interface	citrix_web	Citrix Web Interface	citrix_web	Citrix Web Interface
Citrix Web Access for G/On Menu publication with single sign on	citrix	Citrix Web Interface	citrix	Citrix Web Interface	citrix	Citrix Web Interface
Browser	browser		browser		browser	
Internet Explorer	ie					
Outlook Web Access	owa		owa		owa	
Outlook via http	outlook					
Generic Mail (POP3,IMAP)	generic_mail	Multiport Port Forward	generic_mail	Multiport Port Forward	generic_mail	Multiport Port Forward
Filezilla FTP down/upload	fz	Launch Parameter File	fz	Launch Parameter File	Fz	Launch Parameter File
G/On Help Manager	gon_client_help_manager					
G/On Help Client	gon_client_help					
G/On Management	gon_management					
Secure Desktop					secure_desktop	G/on Secure Desktop
Wake on LAN	generic_wake_on_lan	Wake on LAN	generic_wake_on_lan	Wake on LAN	generic_wake_on_lan	Wake on LAN
Wake on LAN My PC	generic_wake_on_lan_my_pc	Wake on LAN	generic_wake_on_lan_my_pc	Wake on LAN	generic_wake_on_lan_my_pc	Wake on LAN
Wake on LAN Generic	all_fields_wake_on_lan	Wake on LAN	all_fields_wake_on_lan	Wake on LAN	all_fields_wake_on_lan	Wake on LAN
Citrix Generic	all_fields_citrix_web	Citrix Web Interface	all_fields_citrix_web	Citrix Web Interface	all_fields_citrix_web	Citrix Web Interface
Generic single port applications	all_fields_single_port		all_fields_single_port		all_fields_single_port	

G/On 5 Licensing, Pricing and Ordering

G/On Licensing means the process of configuring and obtaining a valid G/On license and installing it.

There are two types of G/On Licenses:

1. A default Demo/Evaluation License
2. A Customer License

The default “Demo/Evaluation License” is included with the G/On 5 installation package and allows G/On to be installed and running for a limited time and with a limited set of options. The “Customer License” is a “normal” G/On license generated and issued as part of the ordering process at Giritech.

The G/On License File

A G/On License is represented by a G/On License File that is generated and issued to customers based on licenses acquired for the number of users (UALs), the number of Tokens (TALs) and the features. A G/On License File is a “flat” text file that can be listed and displayed by the customer for verification of the license. The file is digitally signed by Giritech and cannot be altered.

The box below shows, as an example, the License File for the Demo/Evaluation License:

```
License Number: 0
License File Number: 0
License Timestamp: 2009-10-07T21:13:22Z
Licensed To: G/On Evaluation License - Not for production use
# Dates are in ISO 8601 format YYYY-MM-DD
License Expiration Date: 2010-04-01
Client Connect Address: *
Client Connect Port: *
Number of Gateway Servers: 1
Number of Menu Items: 5
Number of Users: 3
Number of Tokens: 5
Client Platform: Windows
Client Platform: Mac
Client Platform: Linux
Feature: Active Directory User Directory
Feature: Launch Parameter File
Feature: Wake on LAN
Feature: Citrix Web Interface
Giritech Welcome Notification: No license has been purchased for this G/On installation
Giritech Welcome Notification:      ***** EVALUATION PURPOSE ONLY *****
Giritech Welcome Message: No license has been purchased for this G/On installation
Giritech Welcome Message:      ***** EVALUATION PURPOSE ONLY *****
Management Message: This G/On Installation is using a G/On Evaluation License
Management Message: The license is for EVALUATION PURPOSE ONLY and is restricted
Management Message:
Management Message: See www.giritech.com for information on acquiring a license
```

How to obtain a G/On License File

One of the security aspects of a G/On Installation is to ensure the authenticity of the G/On Server by enforcing mutual authentication and preventing the unauthorized duplication of a G/On Server installation and moving it to another location. G/On 3.x was locked to hardware information on the physical server. This approach proved impractical running the G/On server in virtualized server environments. As part of the license in G/On 5 we include the IP Addresses (or DNS names) and the IP Ports used by the G/On Client to connect to the G/On Server. This will prevent a copied G/On Server installation from operating on another IP address.

Consequently, as part of the ordering process, **Giritech must have the IP Address/DNS name and the IP Ports used by the G/On clients to connect.** Initially, Giritech will provide the G/On License file entirely via an off line process. It is our current plan for the future to provide a web based tool for customers and partners to retrieve the G/On License file themselves.

Please Notice: *If a G/On customer has to change the Public IP Address (or DNS name) and/or Public IP Ports for their G/On Gateway servers, a new license file must be generated by Giritech!*

*Also notice: The G/On 5 **Demo/Evaluation** License allows the user or IT administrator to specify the IP Address and Ports and does not require Giritech involvement.*

Successful installation of a valid G/On License File will result in the display of Customer Name during the login process for all users and G/On administrators. If G/On is installed prior to obtaining a valid customer license, G/On will use the default Demo/Evaluation license. An invalidated G/On License File will result in warning messages to users and G/On administrators.

License details overview

A G/On License File reflects the license acquired and issued. The file contains the following information:

Name of license detail	Evaluation license value	Description	Included in a 5.3 License
Installation details			
G/On License Number	0	The primary license identifier. A unique number identifying a specific G/On license. Typically associated with one specific Giritech customer.	Yes
License File number	0	Unique number identifying the specific G/On License File. The "License File Number" is incremented every time a new license file is created associated with a specific G/On License.	Yes
License File Timestamp	-	The date of the creation of the G/On License File. Added by Giritech when the file is created.	Yes
License Date Timestamp	-	A date specifying the date the license was created by ERP system, typically identical to "License File Date". Added by Giritech when the license file is created.	Yes
Licensed To	"Evaluation license – not for production use"	Text identifying the licensee (company name and department). The "Licensed To" information is shown in the welcome page of the G/On Server Configuration and to all users in the G/On Client notification. The default value is the customer company name but can be different as requested by customer or chosen by Giritech.	Provided by customer
Maintenance Expiration Date	-	A date identifying the expiry date of the current maintenance agreement associated with this specific G/On license. This date is renewed annually as part of the maintenance renewal process. During the update of G/On the software release date is compared with the "Maintenance Expiration Date". The update process is terminated if the software release date falls after the Maintenance Expiration Date. <i>Note: G/On cannot be purchased without at least 12 months maintenance. A new G/On installation will therefore always have a valid Maintenance Expiry date.</i>	Yes
License Expiration Date	6 months from product release date	The expiration date of the G/On License. Most G/On Licenses are licensed as perpetual licenses but will always have an expiration date. The demo/evaluation license will expire within 6 months of installation. A customer license with expire five years from purchase. Active licenses will automatically be extended. Non-perpetual licenses will expire according to the subscription period.	Yes

Client Connect IP Address	Configurable	A list of one or more IP addresses/DNS names defined for the G/On Client. This information must be provided Giritech as part of ordering process and prior to the issuance of the G/On License File.	1
Client Connect IP Port	Configurable	A list of one or more IP Ports defined for the G/On Client. This information must be provided Giritech as part of ordering process and prior to the issuance of the G/On License File.	1
HTTP Encapsulation Client Connect Port	None	The IP Port to be used for the G/On Client to connect for HTTP Encapsulation.	0
Feature	Yes Yes Yes Yes	Multiple Client Connect IP Addresses (Yes/No) Multiple Client Connect IP Ports (Yes/No) HTTP Encapsulation (Yes/No) LDAP User Directory (Yes/No) Active Directory User Directory (Yes/No) MS SQL Server Database (Yes/No) Login Notification Mail (Yes/No) Post-login Message (Yes/No) Multiport Port Forward (Yes/No) Launch Parameter File (Yes/No) Wake on LAN (Yes/No) Citrix Web Interface (Yes/No)	No No No No No, but required No No No No No No No No
Number of Gateway Servers	1	Maximum number of G/On Gateway Servers known and managed by one G/On Management server. Default is 1.	1
Number of Users	3	Maximum number of users managed by G/On. Measured in number of User ID's configured in G/On. Licensed by User Access Licenses.	Yes
Number of Tokens	5	The total number of tokens managed by G/On. Licensed by Token Access Licenses.	Yes
Number of Menu Items	10	Maximum number of Menu Items that can be defined. Default is 10 Menu Items in regular licenses.	20

Pricing & End User License Agreement

Note: G/On 5 licensing is governed by the End User License Agreement (EULA) available on www.giritech.com.

Pricing

Giritech's partners can register and log on to Giritech's web site where they will find the G/On 5 pricelist in the Partner section of www.giritech.com.

Upgrade Pricing

Existing customers on an active Maintenance Plan are offered full price protection when they upgrade to G/On 5. The price for an upgrade from G/On 3.x to G/On 5 with similar functionality is calculated as the difference between the new price for the G/On 5 solution and the current maintenance base of the G/On 3.x solution. Existing customers that want to take advantage of G/On 5 now can purchase the upgrade and start implementing G/On 5 for Mac and Linux users and for other users who need the G/On MicroSmart and G/On USB MicroSmart Tokens. Existing Windows users will continue using the existing G/On 3.6 until G/On 5 supports the G/On USB H2 and G/On USB H3 keys used for G/On 3.6.

Ordering

No special order forms will be provided by Giritech. We accept any purchase order formats or email referencing the part number codes and part type codes as listed in the G/On 5 Price List.

G/On Partners outside Denmark can order G/On products, by sending an email to int-orders@giritech.com. G/On Partners in Denmark, please use orders@giritech.com.

Please observe:

1. If you are ordering G/On for a **new customer** please provide full contact details of the customer. That will help us understand our customers and enable us to service you better in the future. For a new customer **ALWAYS REMEMBER:** *You must provide the G/On Client Connect IP Addresses and the G/On Client Connect IP Ports and - if used – the G/On Client HTTP Encapsulation Connect Port.*
2. If you are ordering products for an **existing customer**, please provide enough information about your customer that will enable us to identify the customer. If the customer has multiple G/On licenses, please let us know for which license you are ordering the products by referencing License Number or Licensed-To information. If there are any changes to the Client Connect IP Addresses and Client Connect IP Ports, please remember to include this information in your order request.

The information contained in this document represents the current view of Giritech on the issues discussed as of the date of publication. Because Giritech must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Giritech, and Giritech cannot guarantee the accuracy of any information presented after the date of publication.

This product announcement is for informational purposes only. GIRITECH MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Giritech may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Giritech, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2009 Giritech A/S, Denmark. All rights reserved.

Giritech, G/On, and EMCADS are either registered trademarks or trademarks of Giritech A/S

www.giritech.com