

G/On™ SYSTEM DIAGRAM



G/On USB Token

The G/On USB MicroSmart Token integrates strong 2-factor authentication using 2048 bit smart card generated public/private keypair for the challenge/response protocol. The G/On USB Token includes the G/On Client for convenient mobile connectivity. User name and password is validated against company directory (AD or LDAP).

G/On's virtual connection keeps the user PC off the company network.

Contrary to the conventional direct connectivity on LAN and through VPN tunnels, G/On's client/server architecture creates a protected connection between a client proxy and a server proxy that effectively isolates the PC from the network.

All data is encrypted using FIPS 140-2 validated 256 bit AES – nothing is transmitted in plain text. The G/On Client leaves no footprint on the user PC.

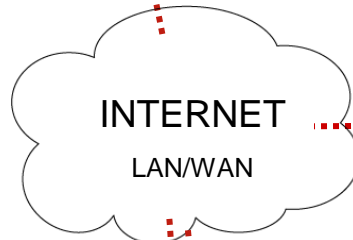
G/On also offers the option of booting directly from the USB Token and load **Secure Desktop**, a locked down Linux operating system that provides a fully managed environment for the secure connection.

G/On Computer Token

As a convenient alternative to the USB Token, the G/On Computer User Token turns the PC into an authentication token.

G/On Mobile Token

Turns an Apple iPad, iPhone and iPod into a personal Token and the G/On Client for iOS provides secure access to corporate applications.



Firewall

Only one port needs to be open for G/On traffic.

Corporate Intranet / LAN

G/On Server (Windows)



Microsoft AD or LDAP

Server based computing

e.g. Microsoft Terminal Server, Citrix, Mainframe, VMware, or easily connect to your office desktop

Client/Server applications

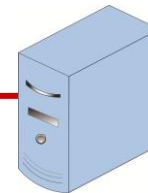
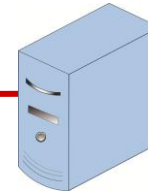
e.g. Outlook, Dynamics NAV, SAP, CRM, Lotus Notes.

Web-based applications

e.g. Intranet, Extranet, Portal etc.

TCP communication

e.g. self- or partner-developed applications.



G/On Server

Software Components

- G/On Configuration – system installation og configuration
- G/On Management – user authentication policies, application authorization policies, and application connectivity configuration
- G/On Gateway Server managing connections and enforcing policies

Hardware requirements

- 2GB available hard disk space
- Minimum 2GHz Processor
- Minimum 2GB memory

Software requirements

- Microsoft Windows Server 2003 R2 SP2
- Microsoft Windows Server 2008 or 2008 R2
- 32 bit and 64 bit

Firewall requirements

- One TCP port for "Through Traffic".

Infrastructure requirements

G/On Server must be a full member of the Domain for Microsoft Active Directory user authentication (Note: G/On does not support Microsoft Windows NT Domain). Full support for LDAP compliant user directories.

Placement

Depending on the desired level of security and performance, we recommend installing a dedicated server for G/On server software. Alternatively, G/On can be installed on:

- Proxy Server
- Terminal Server

We advise against installing G/On on the same server as the AD Server or a Web Server

G/On Client

- 128 MB for minimum configuration. 1GB recommended.
- Microsoft Windows XP (32 bit)
- Microsoft Vista, Windows 7 (32/64 bit)
- Apple MAC OS X 10.6 (Snow Leopard)
- Linux Fedora 14 (32 bit only)
- Apple iOS 4.3

Firewall requirements

Must be open for outgoing traffic on the ports configured in G/On, typically 443 or 80. Supports HTTP proxy.

G/On USB Tokens

G/On USB MicroSmart 1GB

- USB port version 1.1 and higher
- Min. one virtual drive mapping available (e.g. drive E:\)
- Supports Windows, Mac, Linux

G/On USB H3 1GB

- USB port version 1.1 and higher
- Min. two virtual drive mappings available (e.g. drive E:\ and F:\)
- Supports Windows only
- Requires administrative rights for remote update of CD partition

G/On Computer User Token

Hardware requirements

- 1GB available hard disk space

Software requirements

- Windows only

G/On Mobile Token

Requirements

- Apple iPad, iPhone & iPod with iOS 4.3+

Connectivity

G/On supports TCP connectivity such as RDP (Microsoft) and ICA (CITRIX) for remote desktop and other client/server applications

Verification

Secure Key Exchange and mutual two-factor user authentication based on 2048-bit Public Key Cryptosystem Scheme RSAES<OAEP<SHA1>>

Encryption

FIPS 140-2 Validated 256-bit AES data encryption

Core Technology

G/On is built upon Giritech's patented technology and method called EMCADS™ (Encrypted Multipurpose Content and Application Deployment System)

Tested Application Clients

G/On has been tested with, and fully supports the following:

- **Microsoft® Exchange** 2003 using Outlook 2003, Outlook 2007, and Outlook 2010 clients
- **Citrix®:** Server side single sign on, Citrix farms, published applications
- **Microsoft® Windows® Terminal Server:** Server side single sign on, Remote Apps, Connection Broker,
- **Browser:** G/On supports most of the commercially available browsers. Giritech recommends using Microsoft Internet Explorer®. If application is Java-based, no specific browser is required. Note that Microsoft® Internet Explorer does not provide out-of-the-box Java support, separate installation is required.

Custom-made Solutions

Giritech's Partners have configured and tested a long list of application interacting with G/On. Amongst these are:

- **ERP:** Microsoft Dynamics (AX, NAV, C5) and SAP
- **Mail:** Lotus Notes
- **Remote Desktop and Application Access:** VNC and VDI
- **Database:** Database Client Applications (Oracle, MS-SQL, DB2)
- **Other Terminals and Emulation:** PuTTY for SSH & Telnet and Mocha for 3270 & 5250
- **File Sharing:** FileZilla access to FTP server, WebDAV access Microsoft SharePoint

G/On™

For more information please visit

www.giritech.com