

**GIRITECH®**



**G/On™**  
**Secure Virtual Access Solution**



# Secure Mobile Access



**From everywhere...**



**From any device...**

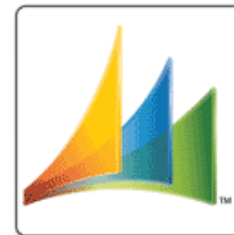


**From user...**

**...to applications**



**...without  
compromising on  
security  
and  
usability**



... and to my PC in  
the office:



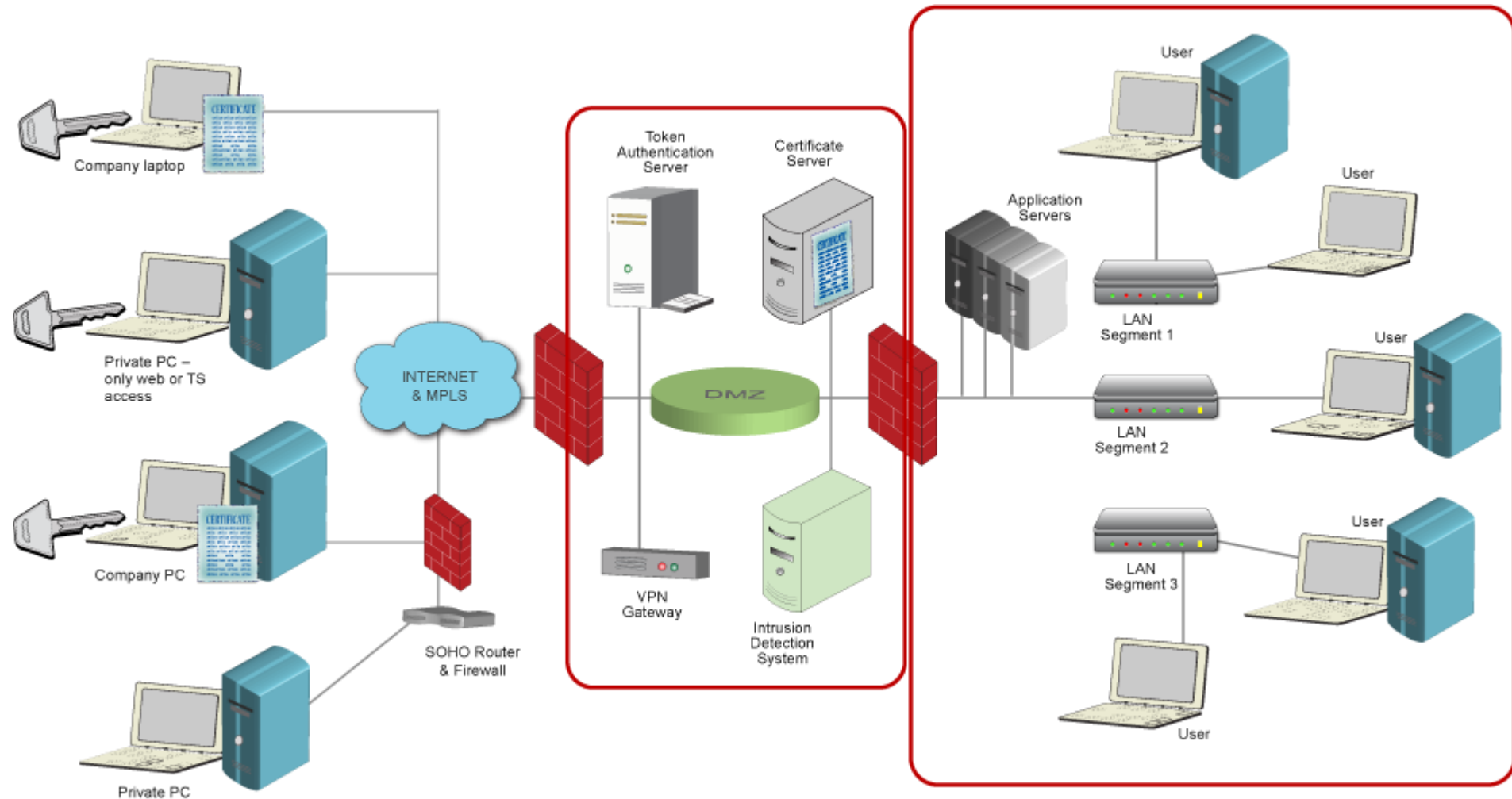
# Secure Virtual Access

Contrary to direct access and VPNs,  
G/On does **NOT** make user devices  
part of the company network

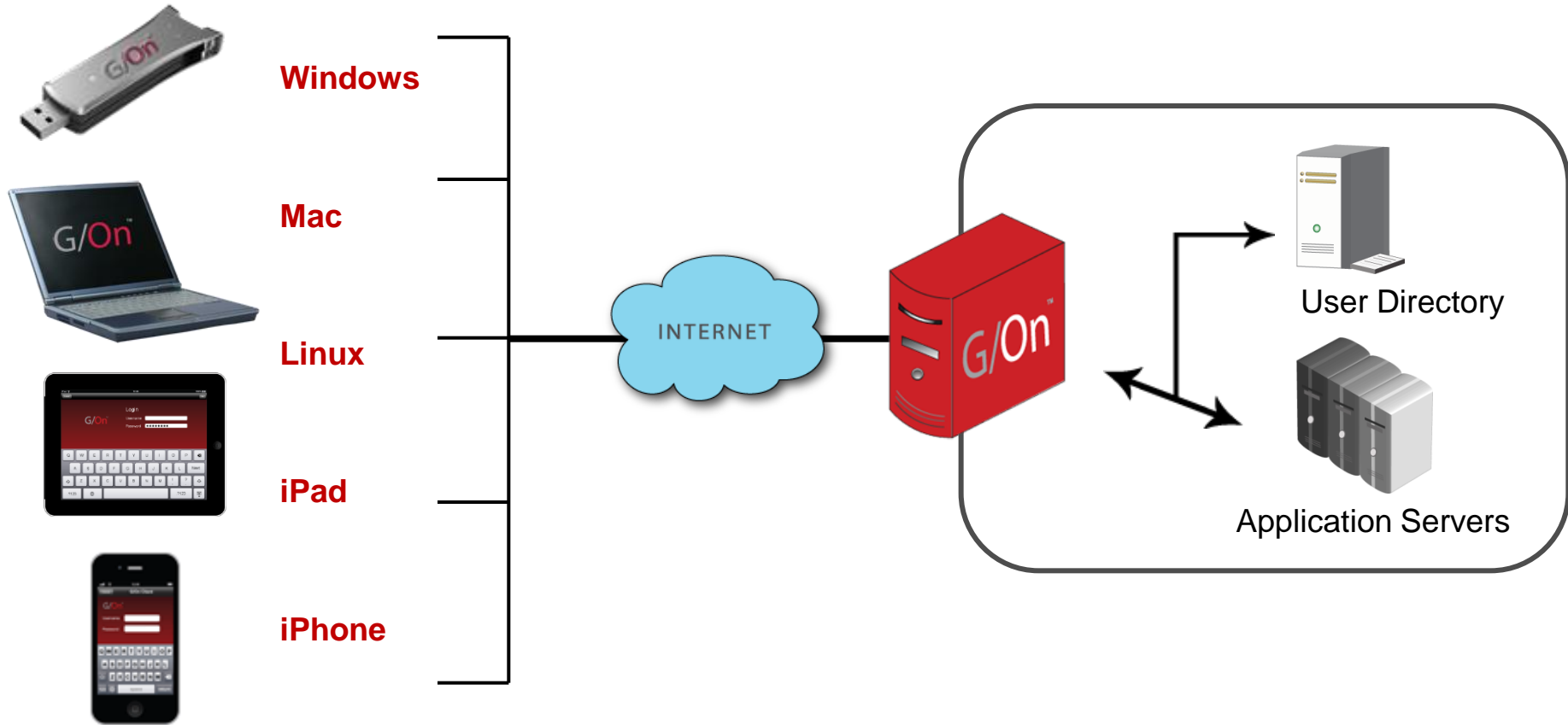
G/On creates  
**virtual connections**  
between users and applications

G/On is a client/server software solution implementing  
a distributed port forwarding proxy with integrated security.

# Get away from this...



# ... and use this



The **G/On Client** is deployed on multiple platforms and formats and provides easy access to the applications

The **G/On Gateway Server** controls all access to the Application Servers

# Why do customers buy G/On?

**”G/On makes mobile security simple!”**

**For different people**



- Employees**
- Telecommuters**
- Customers**
- Partners**
- External Contractors**
- ...**

**Using different devices  
in different locations**



- Home PCs**
- Branch Offices**
- Partner Offices**
- Customer Offices**
- ...**

**To quickly and securely  
access corporate  
applications**



- My PC Desktop**
- Terminal Server/Citrix**
- Email**
- Specific Applications**
- Intranet**
- File Shares**
- ...**

# One single integrated solution

Hardware token for integrated **2-factor** authentication and **secure virtual connectivity**

- **USB Tokens** with integrated smart card and storage for the G/On Client, **or**
- **Computer User Tokens** combining hardware info and software generated keypair (available for PCs and mobile devices like **iPad** and **iPhone**)

Authentication is **mutual** to prevent man-in-the-middle attack

- Public/private key cryptography (RSA keys), like certificates, but without the complexity of X.509 and without the need for Public Key Infrastructure (PKI).

User name and password validated against existing company directory (AD, LDAP)

- Offers single sign-on (SSO) experience for most applications

USB Tokens for use on any **Windows**, **Mac** and **Linux** device

- Use any computer anywhere to get secure access to corporate applications, office PC, desktops, Citrix, ERP, Intranets, web apps, and other services
- **Mobile flexibility** without driver and software installation

# One single integrated solution

256bit AES encrypted, **virtual** connections for data in transit

- Each application gets its own encrypted connection
- FIPS 140-2 compliant encryption on Windows client platform

Application authorization based on AD, LDAP policies, circumstance & device

## **Bootable USB option**

- With locked down Linux-based G/On OS operating system on USB
- Provides full independence and isolation from PC hard disk
- Managed client environment

Enterprise architecture for management, availability and scalability

- Centralized management of policies, user tokens, and application access
- Tools for managing token software, deployment and enrollment

# Enterprise Security on iPhone & iPad

G/On Client for iOS, App Store Edition (free download)

Secure access to web applications

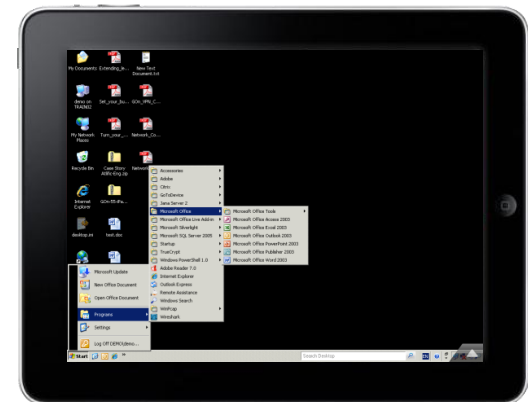
Secure access to Remote Desktop on your office PC or Terminal Server farm

## Leverage existing, corporate web applications

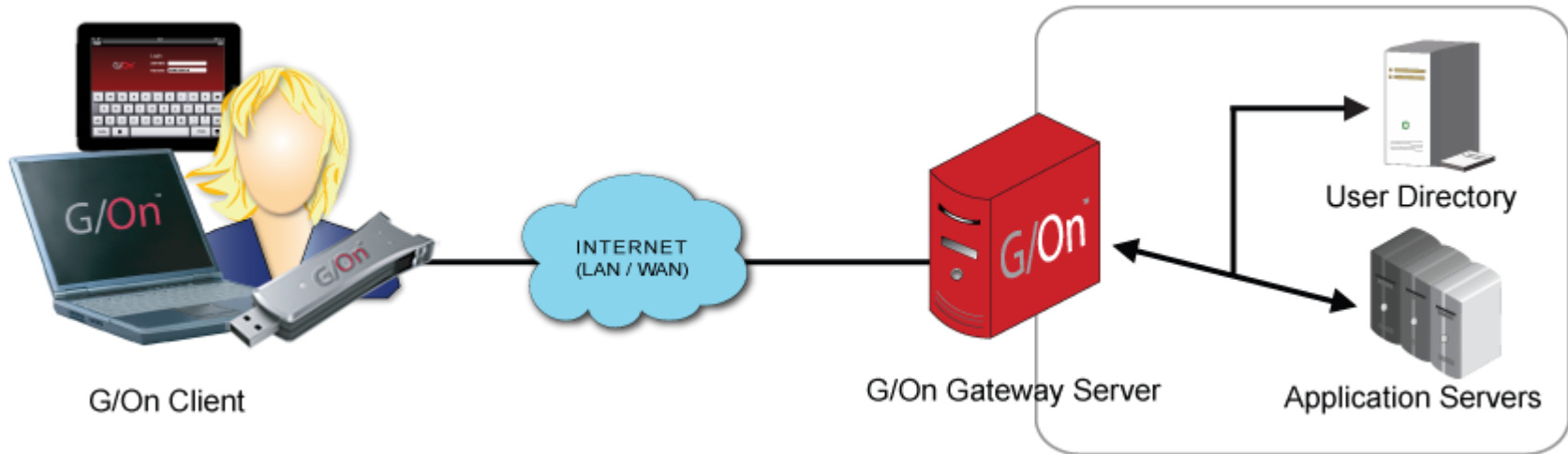
- iPad and iPhone access to webmail, intranets, portals, and other company web apps
- Using built-in secured G/On browser based on iOS WebKit framework
- Offers single sign-on managed by the G/On Server (depending on configuration)
- Individual, isolated browser sessions with encrypted connections to specific web apps
- Each browser session managed by the G/On Server
- No data left on the device and no access from the iPad/iPhone Safari browser

## Access to your office PC desktop and Terminal Server farms

- Use your favorite Remote Desktop (RDP) client on iPad/iPhone \*)
- Single sign-on managed by G/On Server
- Access to all your tools and data as if you are in your office
- No password data on the device
- No corporate data on the device



# Easy to use – Easy to manage



## A single menu interface for the user

My Office PC
My Desktop on Server
MS Word on Citrix
MS Excel on Citrix
Download/Upload Documents
ERP (Dynamics)
CRM (Dynamics)
Intranet Portal
Expense Reporting
E-Mail on Citrix
E-Mail (OWA)
E-Mail – My Local Outlook
About G/On
Exit

## Mutual, 2-factor user and client/server authentication via

- **Challenge/Response protocol for token/server identification**
- **User directory for User ID and Password validation**

## The G/On Server authorizes the user for applications

- **By user group membership**
- **Defined by the G/On administrator**

## Applications are defined

- **Via Menu Action Templates on the server**
- **User menu is dynamically created by server at logon**

## A single tool for the administrator

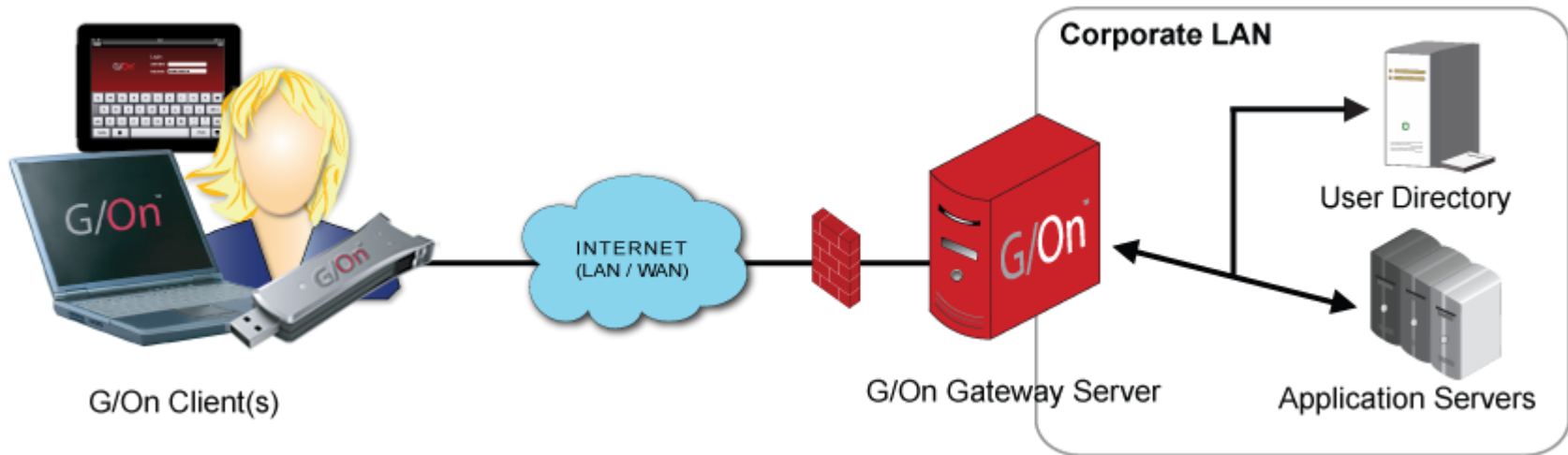
- **Office PCs/Virtual Desktops**
- **Server-based computing**
  - Citrix/MS TS/VMWare
- **FTP Server**
- **Client/Server apps**
  - SAP, Dynamics, etc
- **Web apps**
  - Intranet, Xtranet
  - Doc management
  - Specific apps
- **Mail & Collaboration**
  - Exchange
  - Notes
- **Database Applications**

**G/On™**

**Deployment & Management**

# Deployment & Management

Typically for smaller organizations



## A single menu interface for the user

My Office PC
My Desktop on Server
MS Word on Citrix
MS Excel on Citrix
Download/Upload Documents
ERP (Dynamics)
CRM (Dynamics)
Intranet Portal
Expense Reporting
E-Mail on Citrix
E-Mail (OWA)
E-Mail – My Local Outlook
About G/On
Exit

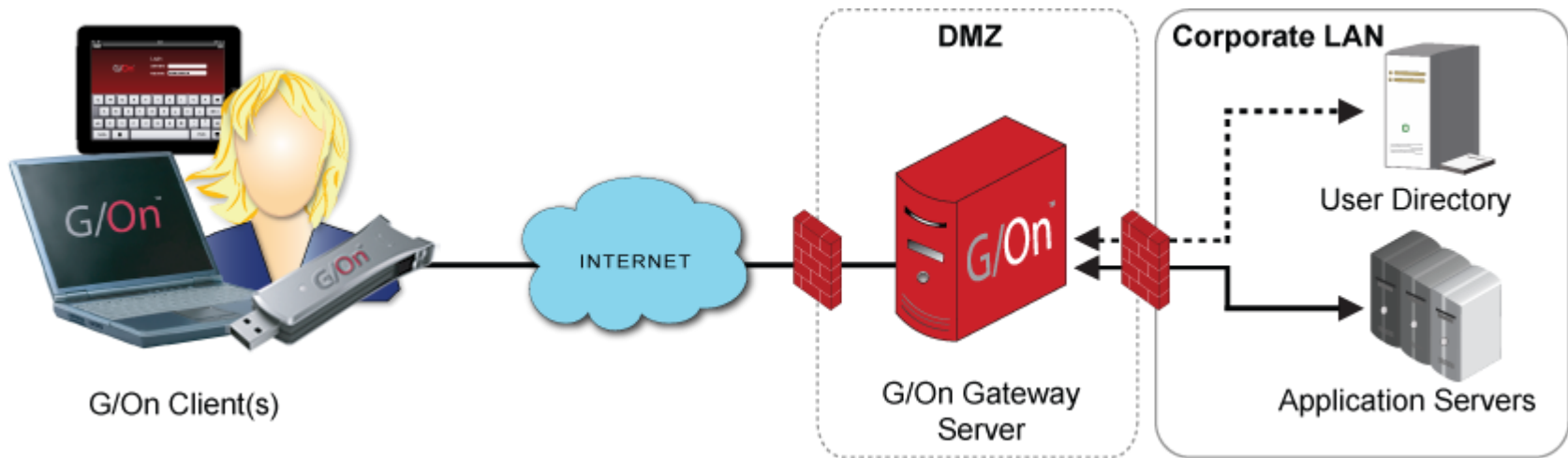
- Easy to implement
- Easy to manage
- Maximum agility
- Offers a low cost of entry

## A single tool for the administrator

• Office PCs/Virtual Desktops
• Server-based computing
• Citrix/MS TS/VMWare
• FTP Server
• Client/Server apps
• SAP, Dynamics, etc
• Web apps
• Intranet, Xtranet
• Doc management
• Specific apps
• Mail & Collaboration
• Exchange
• Notes
• Database Applications

# Deployment & Management

## Typical Enterprise configuration



### A single menu interface for the user

My Office PC My Desktop on Server
MS Word on Citrix MS Excel on Citrix
Download/Upload Documents
ERP (Dynamics) CRM (Dynamics)
Intranet Portal Expense Reporting
E-Mail on Citrix E-Mail (OWA) E-Mail – My Local Outlook
About G/On Exit

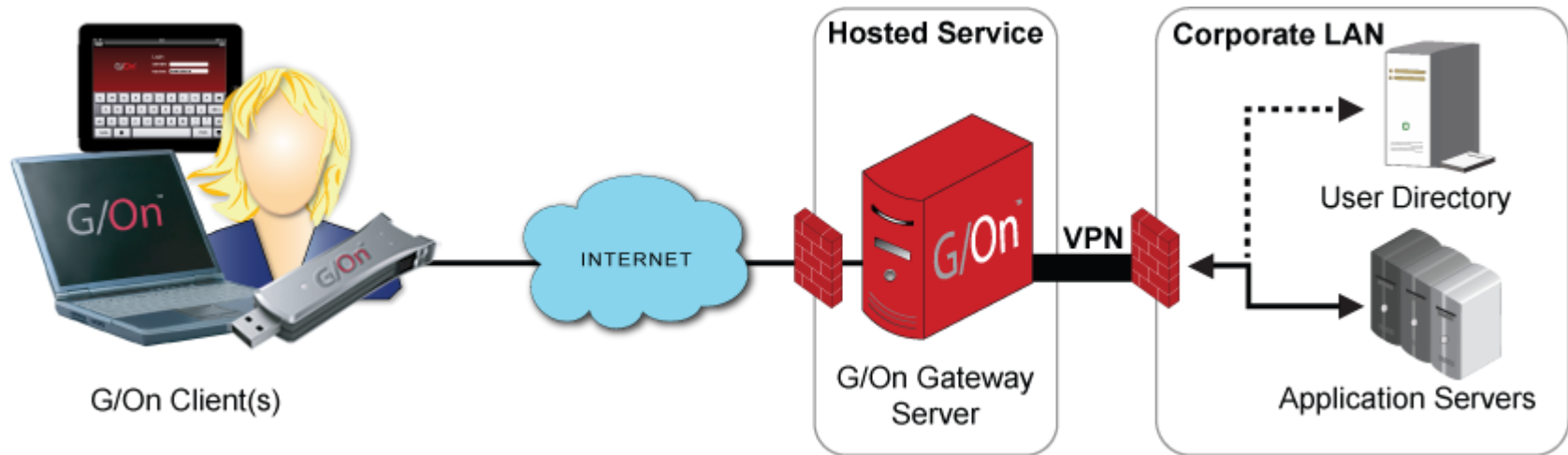
- Enables compliance with typical enterprise security and control policies
- Integrates and co-exists with existing technologies for remote access

### A single tool for the administrator

• Office PCs/Virtual Desktops
• Server-based computing <ul style="list-style-type: none"> <li>• Citrix/MS TS/VMWare</li> </ul>
• FTP Server
• Client/Server apps <ul style="list-style-type: none"> <li>• SAP, Dynamics, etc</li> </ul>
• Web apps <ul style="list-style-type: none"> <li>• Intranet, Xtranet</li> <li>• Doc management</li> <li>• Specific apps</li> </ul>
• Mail & Collaboration <ul style="list-style-type: none"> <li>• Exchange</li> <li>• Notes</li> </ul>
• Database Applications

# Deployment & Management

## G/On as a Managed Service



### A single menu interface for the user

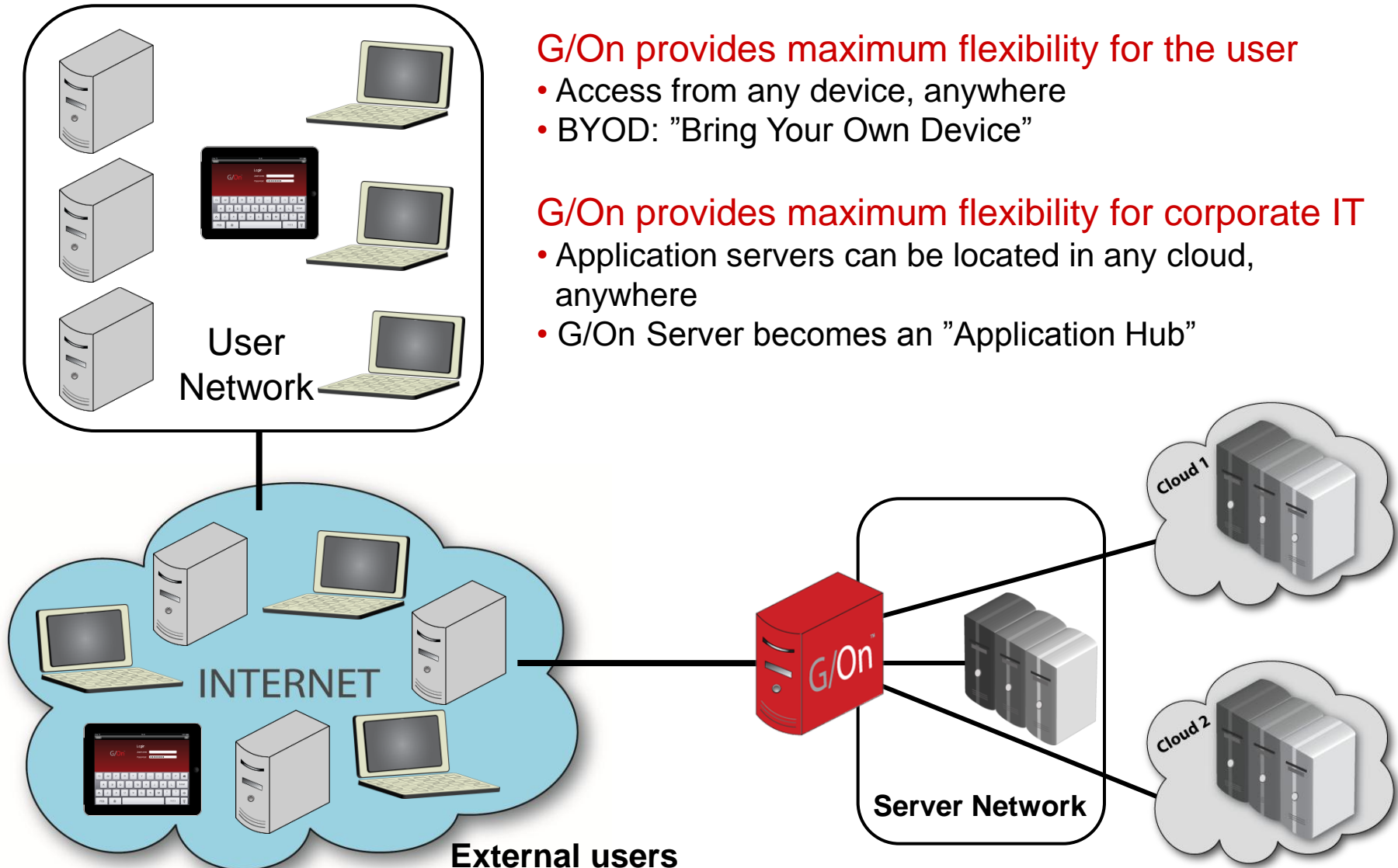
My Office PC My Desktop on Server
MS Word on Citrix MS Excel on Citrix
Download/Upload Documents
ERP (Dynamics) CRM (Dynamics)
Intranet Portal Expense Reporting
E-Mail on Citrix E-Mail (OWA) E-Mail – My Local Outlook
About G/On Exit

- Offers additional simplicity for customer
- Fully managed by service partner
  - Token management
  - Application access
- Maximum control
- Defined levels of service of quality
- Defined levels of support

### A single tool for the administrator

- Office PCs/Virtual Desktops
- Server-based computing
  - Citrix/MS TS/VMWare
- FTP Server
- Client/Server apps
  - SAP, Dynamics, etc
- Web apps
  - Intranet, Xtranet
  - Doc management
  - Specific apps
- Mail & Collaboration
  - Exchange
  - Notes
- Database Applications

# G/On & "The Cloud"



**G/On provides maximum flexibility for the user**

- Access from any device, anywhere
- BYOD: "Bring Your Own Device"

**G/On provides maximum flexibility for corporate IT**

- Application servers can be located in any cloud, anywhere
- G/On Server becomes an "Application Hub"

**G/On<sup>™</sup>**

# Authentication Tokens

# Secure authentication

---

## Challenge/Response protocol

- Industry standard method
- Using public/private key cryptography (RSA keys), like certificates, but without the complexity of X.509 and without the need for Public Key Infrastructure (PKI).
- See [http://en.wikipedia.org/wiki/Public-key\\_cryptography](http://en.wikipedia.org/wiki/Public-key_cryptography)

## Types of authentication Tokens:

### Hardware tokens with smart card

- Maximum Strength Authentication
- Private key generated, stored and kept secret inside hardware
- Software inside hardware token implements the Challenge/Response protocol
- *G/On smart card tokens: No installations, no drivers*

### Hardware tokens without smart card

- Private key generated by user PC and **linked/locked** to PC or device
- Software on the user PC implements the Challenge/Response protocol

### Software tokens

- Private key generated by user PC and stored on PC or device
- Software on the user PC implements the Challenge/Response protocol

# Hardware Tokens with smart card

---

**G/On integrates 2-factor, mutual authentication**

- **Smart card based authentication tokens**
- **Includes 1GB storage for the G/On Client**
- **For Windows, Mac, Linux**
- **No special drivers required**



**G/On MicroSmart**

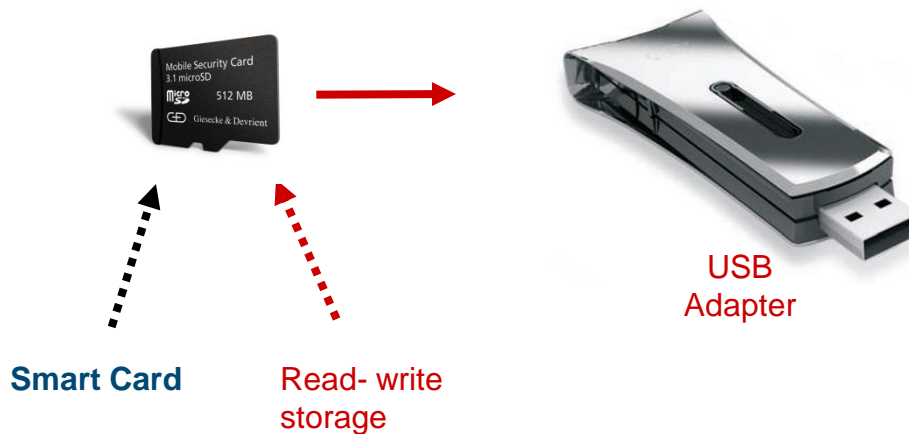


**G/On USB MicroSmart**

# G/On MicroSmart Token

The **ultra versatile** solution with 2-factor Smart Card Authentication for Windows, Mac and Linux users

This MicroSD with integrated Smart Card for authentication and G/On Client for connectivity provides the most versatile and flexible secure remote access solution in the world!

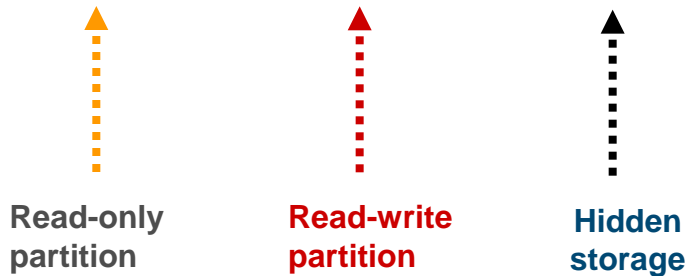


**G/On™**

**Hardware tokens  
without smart card**

# G/On USB H4 Token

## Token for Windows users with the convenience of a CD drive



*Will be phased out when G/On USB SafeSmart is available.*

**Integrated CD-ROM for auto-launch and read-only protection of the G/On software**



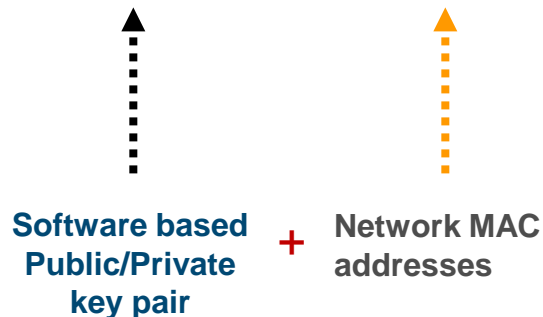
Authentication based on Private key stored in hidden memory and linked to unique ID.

An affordable token for Windows users with the convenience of auto-launch and the read-only protection of the G/On client software.

# G/On Computer User Token

(G/On Mobile Token on iPhone & iPad)

## The convenient solution for users with personal devices



The device becomes a hardware authentication token



Authentication based on Private key stored in registry combined with network MAC-addresses and/or unique device ID. Information is stored in protected area under iOS

The G/On client, the token and application clients are installed directly on the device under the user account.

# Client Side Options

---

## Support for different security policies:

- **Launch of G/On Client from user's USB token**

User plugs in the G/On USB Token and launches the G/On client. CD partition provides auto-launch

- **Launch of G/On Client installed on user's device**

User's device is enrolled as authentication token

- **Boot of PC from user's USB token**

User can boot a locked down Linux-based G/On operating system from the G/On USB and **achieve a managed and known environment on an unknown PC**

# Boot of PC from G/On USB Token

---

## G/On OS

- Turns an unknown PC into a **known** and **managed** device
- Boots from the G/On USB Smart Token
- Loads a G/On specific, hardened Linux operating system
- Can only connect to the corresponding G/On Server
- Provides a Linux desktop
  - Configuration of network connections (Cable/Wireless/Mobile Broadband)
  - Browser (Firefox)
  - Rdesktop for Remote Desktop Access through G/On
  - Citrix ICA client for Citrix access through G/On
  - Filezilla for FTP file upload and download via G/On
  - Access to a minimum set of standard Linux tools
- An ideal, cost-effective option for many organizations:
  - With a policy for access from managed devices only
  - Looking for the ultimate secure solution
  - For instance: Local & Federal Government, Police, Banks, Law firms, Accountants, ...



...NOW ALSO FOR LINUX

# Client Side Features

---

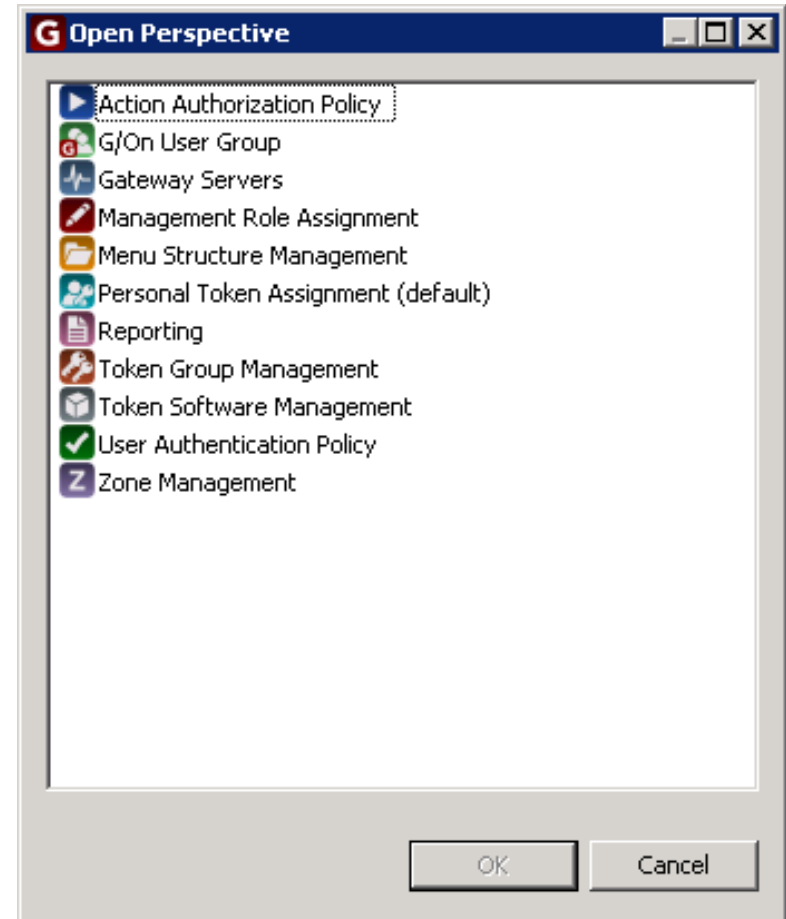
Help the user behave responsibly, and lower the risk of accidental misuse:

- **Support for AD/LDAP password change during G/On login**
- **Automatic disconnect after period of inactivity**
- **Closing of connections and programs, when the token is removed**
- **Closing of connections that are not to be used anymore, when a user closes the application**
- **Lock-2-Process between application clients and their connections though G/On**

# A Single Point of Management

## One single tool

- Authentication policies
  - Right Person
- Authorization policies
  - Right Application
- Zones
  - Right Circumstances
- Application provisioning
  - Right Access
- Reporting



# Authentication

- Authentication Tokens
- Users
- Authentication Rules

The screenshot displays the 'G/On Management' application window. The main pane is titled 'Personal Token Assignment' and shows a list of 25 items. The left pane shows a list of 58 users. The main pane table is as follows:

Token	User	Personal Token Status
ComputerUserToken-0002	bsh@giritech.com	Personal Token
ComputerUserToken-0003	rs@giritech.com	Personal Token
ComputerUserToken-0004	rs@giritech.com	Personal Token
ComputerUserToken-0005	twa@giritech.com	Personal Token
ComputerUserToken-0006	bsh@giritech.com	Personal Token
HagiwaraH4-0001	bsh@giritech.com	Personal Token
SoftToken-0001	bsh@giritech.com	Personal Token
SoftToken-0002	bsh@giritech.com	Personal Token
SoftToken-0003	bsh@giritech.com	Personal Token
SoftToken-0004	bsh@giritech.com	Personal Token
mobile-0012	jpo@giritech.com	Personal Token
mobile-0013	emo@giritech.com	Personal Token
mobile-0014	twa@giritech.com	Personal Token
mobile-0015	twa@giritech.com	Personal Token
mobile-0016	pwl@giritech.com	Personal Token
mobile-0017	rs@giritech.com	Personal Token
mobile-0018	jpo@giritech.com	Personal Token
mobile-0019	bsh@giritech.com	Personal Token
mobile-0020	jt@giritech.com	Personal Token
mobile-0021	rs@giritech.com	Personal Token
mobile-0022	cso@giritech.com	Personal Token
mobile-0023	rs@giritech.com	Personal Token
mobile-0024	jt@giritech.com	Personal Token
mobile-0025	zg@giritech.com	Personal Token
mobile-0026	zg@giritech.com	Personal Token

The left pane shows a list of users, including: \$jpo@giritech.com, AVexec@giritech.com, Administrator(@giritech.com), BGDK1@giritech.com, BGDK2@giritech.com, BackupSvc@giritech.com, Bettina@giritech.com, EUQ\_DUDLEY@giritech.com, IUSR\_DUDLEY(@giritech.com), IUSR\_PAIN(@giritech.com), IWAM\_DUDLEY(@giritech.com), IWAM\_PAIN(@giritech.com), MOMexec@giritech.com, NFH@giritech.com, visma2@giritech.com, boardroom@giritech.com, bsh@giritech.com, bshtest@giritech.com, cgit@giritech.com, chs@giritech.com, crm-acc@giritech.com, cso@giritech.com, dd@qiritech.com.

All user data received successfully

# Authorization

- User Groups
  - From AD/LDAP
  - G/On Groups
- Applications
- Authorization Rules
- Optional:
  - Token Groups

The screenshot displays the G/On Management interface. On the left, the 'Menu Actions' pane shows a list of 82 actions, with '(i) enable RDP w/SSO to my pc1 on ...' selected. The main window shows the 'Action Authorization Policy' configuration for 65 of 65 rules. The table below summarizes the visible data from the main window.

Authentication Status	User Group	Menu Action
✓ Authenticated		(W) Citrix Web Interface x-men
✓ Authenticated		(L) test firefox
✓ Authenticated		(W) Citrix XML x-men
✓ Authenticated		(W) File Server bishop - type 0
✓ Authenticated		(W) Network Drive dev-test-g-on-3
✓ Authenticated		(W) mstsc w/o sso x-men
✓ Authenticated		(W) Nutsmail in Firefox
✓ Authenticated		(W) Remote Desktop on vtst-sos5
✓ Authenticated		(W) Remote Desktop on x-men w/o SSO
✓ Authenticated		(W) FreeRDP hulk
✓ Authenticated		(W) GTSC x-men
✓ Authenticated		(W) FreeRDP x-men
✓ Authenticated		(W) Screen Sharing on "My PC"
✓ Authenticated		(W) Network Folder bishop/dev
✓ Authenticated		(W) Network Drive Q: Bishop/dev
✓ Authenticated		(W) Portforward for network Folder on Q:
✓ Authenticated		(W) Mantis (Firefox, launch type 7)
✓ Authenticated		(M) OWA though Firefox
✓ Authenticated		(W) Mantis (IE, launch type 0)
✓ Authenticated		(W) Nutsmail
✓ Authenticated		(W) Mantis
✓ Authenticated		(i) Nutsmail
✓ Authenticated	bshtest	bsh test2
✓ Authenticated		(W) G/On Management
✓ Authenticated		(M) Screen Sharing on "My PC3" (10.5-.)
✓ Authenticated		(W) Remote Desktop on x-men

All menu action data received successfully

# Application Provisioning

## Applications are provisioned via Menu Actions:

- Multiple Menu Action templates (wizards)
- Server side connectivity to application servers
  - Application server IP/DNS
  - Application server port(s)
- Client side connectivity
  - Client port(s)
- Client side application
  - Application client to be launched
  - Parameters

The screenshot shows a window titled "G All fields, launch type: RDP Connection". The main content area is titled "(i) enable RDP w/SSO to my pc1 on 3389". Below this, there is a form with the following fields and values:

Name	(i) enable RDP w/SSO to my pc1 on 3389	
Menu Title	My Office PC (Enable)	
Menu Image ID	remote_desktop_portforward	
Server Host	%(user.my_pc_1)	Scan network
Server Port	3389	
Client Host (see mouse-over tooltip)	127.0.0.1	
Client Port	3389	
Command		
Close Command		
Working directory		
Lock to process PID	<input type="checkbox"/>	
- or its sub processes	<input type="checkbox"/>	
Lock to process name		
Close with process	<input type="checkbox"/>	

At the bottom right, there are two buttons: "Finish" and "Cancel".

# Reporting

**G/On Management**

File Switch To View Help

Reporting Zone Management Gateway Servers Menu Structure Management G/On User Group Personal Token Assignment Action Authorizati >>

Reporting Export

**Report selection**

- Amount of Usage
- Current User Activity
- Latest Errors
- Latest User Activity
- User Activity between dates**
- User Activity by month

**Report**

User Login: rs@giritech.com  
 Email:  
 External User ID: S-1-5-21-2981504786-2415913618-1285249951-1210

**Session**

Session Start: 24/05/2011 23.33  
 Session End: 25/05/2011 00.39  
 Client IP: 87.60.125.34  
 Server SID: 72c0129e-825b-11e0-80ec-000d601cc98e  
 Unique Session ID: 20110524T233340.826964\_\_102

**Authorization**

**Actual Authorization and Zone Properties**

Authentication Status: Authenticated  
 Management Role: Administrator  
 Mobile: mobile-0023  
 Operating System: safe  
 State:  
 Personal Token Status: Personal Token  
 User: rs@giritech.com

**Authorized Menu Actions**

(L) Access to File Server

**G/On™**

# Solution Scenarios

# G/On 5 Solutions (1 of 3)

---

## Working from home

- **Using "my home PC" or "my iPad" to get to the desktop of "my office PC"**
  - And/or get access to virtual desktops, Citrix, Terminal Server, client/server apps
- **G/On 5 offers Wake-on-LAN so your office PC can "go-to-sleep"**

## Continuity of Operations

- **G/On scales easily and cost-effectively to all employees**
- **You need to give employees a G/On USB only – not a PC**
- **All employees will achieve the flexibility and freedom they are looking for**

## Secure access for external contractors

- **External users can use their own PC to connect to specific applications**
- **Give them a G/On USB and they have access within minutes rather than months**
- **Reduce complexity and cost significantly**

# G/On 5 Solutions (2 of 3)

---

## **G/On Travel Solutions:**

### **1. When you travel without a laptop - use a PC with an Internet connection**

- In the offices of your customers/vendors/partners
- In other trusted environments

### **2. When you travel – bring along an iPad or thin client laptop**

- Leave the PC "clean" – don't take company data on the road
- Preferably with a built in 3G modem for a convenient "Internet everywhere"
- Always use G/On to connect securely to your desktop or other applications
- Never leave data on device – data may end up in the wrong places
- If you lose the iPad/netbook/thin client laptop – just get a new one from a local store

### **3. When you travel with your own laptop**

- Use any Internet connection, or
  - Use built in 3G modem, or
  - Bring your data modem or use your mobile phone as modem
    - You may use G/On MicroSmart in your USB modem or directly in your laptop
- Synchronize mail with your local Outlook/Notes

# G/On 5 Solutions (3 of 3)

---

## **Companies requiring known and managed PCs can avoid the cost of laptops**

- G/On OS is a known and managed Linux operating system
- Provides a "PC on a USB" including G/On secure connectivity
- Cost savings are significant compared to a laptop for all employees

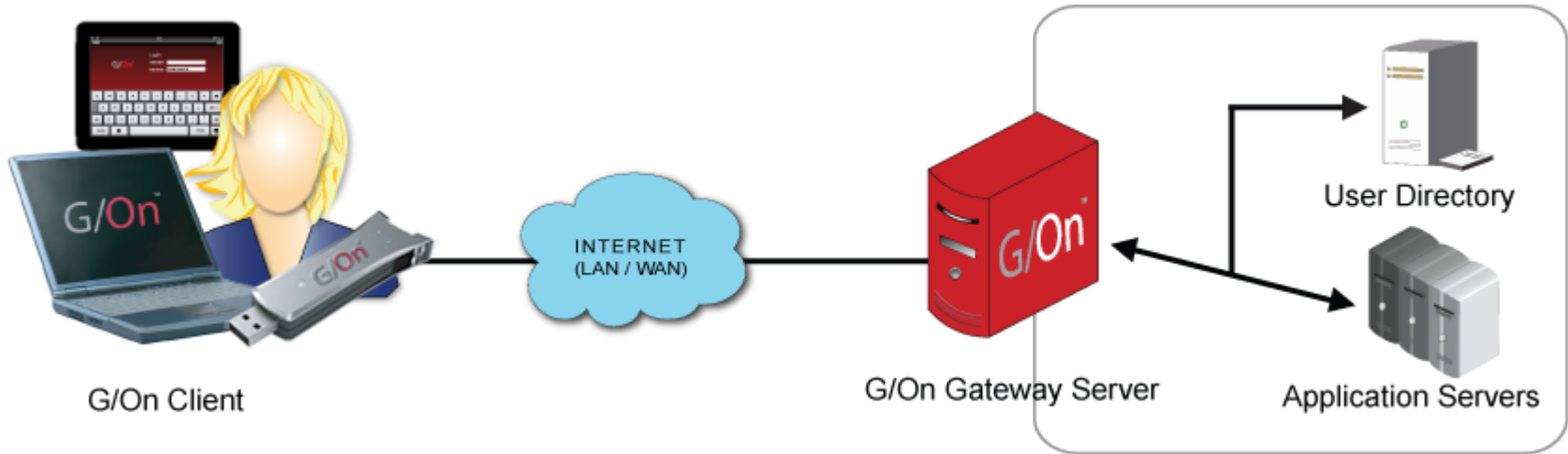
## **Companies can use G/On to secure the wireless network on their premises**

- All connections go through G/On. Only known users will get access
- Users can get access to company applications via the G/On remote access

## **Students can bring their own PC to school and connect to a wireless network**

- All connections go through G/On. Only known users will get access
- Connect students to the Internet through G/On – and let G/On do the logging
- Use G/On to give students access to specific resources on the school network
- Students can bring Windows PCs, Macs, Linux PCs, and iPads

# G/On Minimum Requirements



1. G/On
2. Windows Server 2003/2008
3. Fixed external IP or DNS name
4. One open port in firewall
5. Office PCs

# G/On Value

---

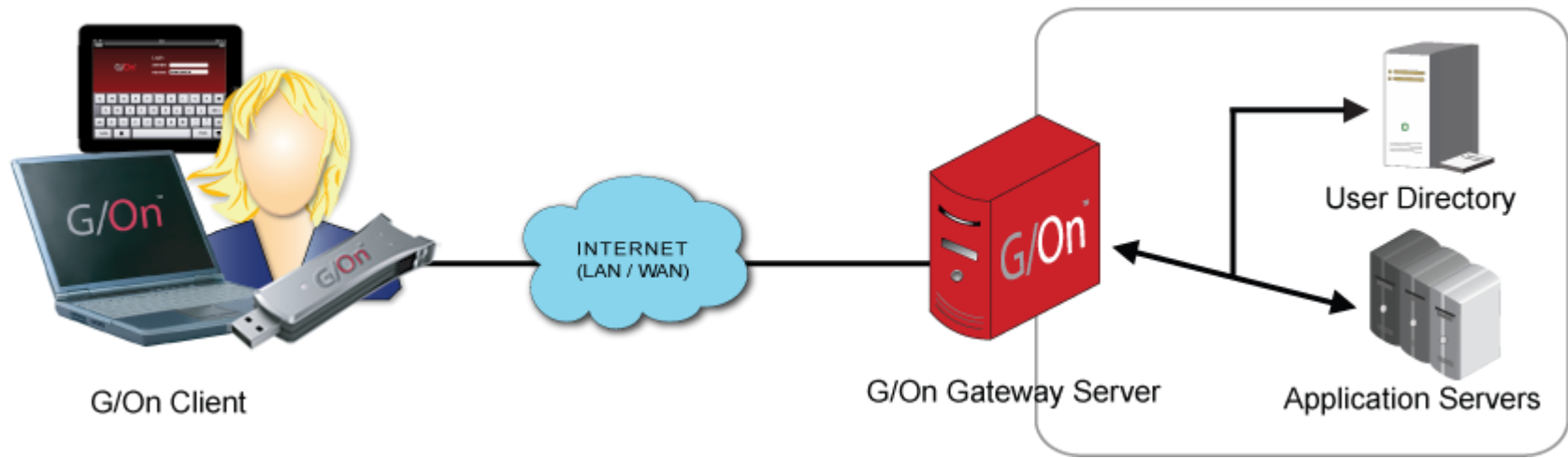
- One simple solution for secure access for
  - All users
  - All user devices
  - All applications & services
- Centrally managed via policies:
  - Authentication policies (the right people)
  - Authorization policies (the right applications)
  - Device policies (right circumstances)
- Providing:
  - Security transparency
  - Lower total cost of ownership
  - Increased flexibility and productivity
  - Positive user experience

## G/On Benefits

G/On helps our customers improve their business:

- Increase productivity
- Enhance employee satisfaction
- Reduce IT costs
- Improve overall security

# Benefits for User & Corporate IT



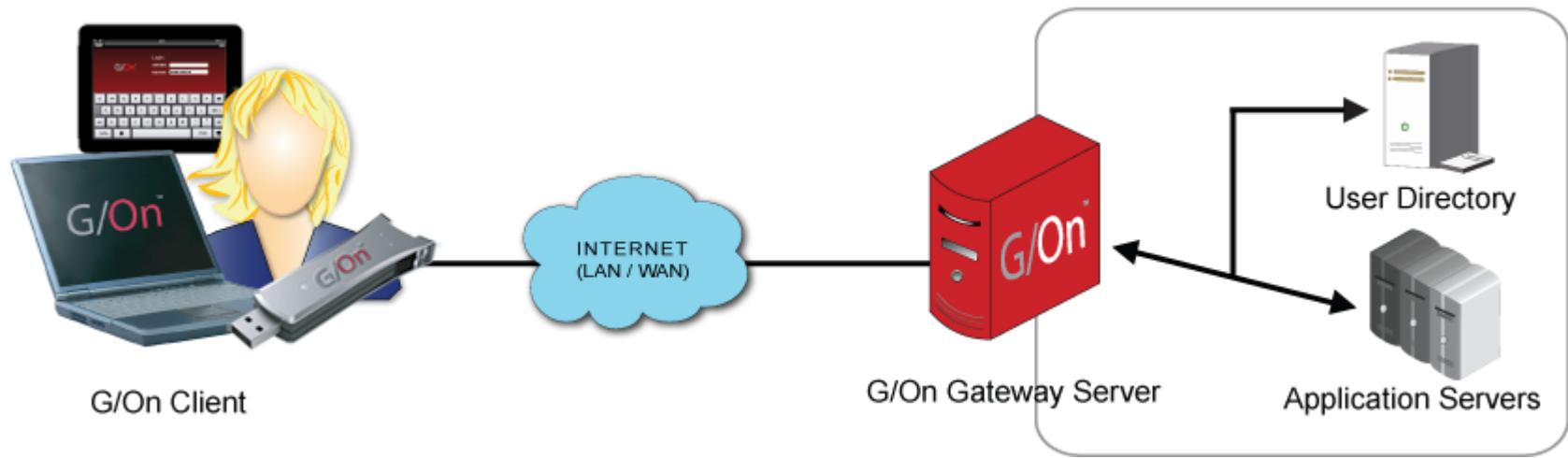
## Benefits for user

- Users can choose Windows, Mac, Linux, iPad, iPhone
- Easy to learn – easy to use
- Nothing to install on PC
- Leaves little room for user mistakes
- No need to remember URLs
- Single sign-on
- One clear menu of applications – One click
- Convenience of auto-launch, say, mail.
- Increased productivity, better work/life balance
- Increased flexibility and job satisfaction

## Benefits for corporate IT

- Enterprise security for iPad & iPhone
- User device is not part of the network
- End point management is not required
- Operating system managed by vendor
- Application clients managed by G/On
- Centralized client sw deployment
- Simplified infrastructure
- Easy to install & configure
- Runs on virtual & physical servers
- No need for additional load balancers
- One tool for Citrix, TS, web apps, office PC's, virtual PC's, client/server apps

# Benefits for IT Security & Customer



## Benefits for IT security/administrator

- Enterprise security for iPad & iPhone
- One, integrated & central solution for secure access
- Single point of policy management
- Policies defined in terms of users and applications – and not in terms of network segments, IP addresses, Ports, filters, etc.
- Integrated 2-factor, smart card authentication
- Integrated application authorization
- Integrated application delivery
- FIPS validated 256 bit AES encryption
- Alternative client options for security, including a hw-independent boot of PC
- No end-point security issues (device stays off the network)
- New applications enabled in minutes

## Benefits for customer

- Simplified, consolidated infrastructure
- Reduced cost – lower TCO
- Tokens do not expire
- PC can be used as token
- "Peace of mind" - State-of-the-Art, integrated security
- One vendor
- Remote access scales to all staff – Business Continuity/Emergency Readiness
- Staff can use home PC for access to work
- Staff can use iPad and iPhone

**G/On™**

**Licensing**

# G/On Standard Configuration

## Additional features are optional

- **Windows, Mac, Linux, and iOS clients**
- **Integrated security**
- **FIPS 140-2 validated 256bit AES encryption**
- **2-factor, mutual authentication**
  - A User Directory either Microsoft Active Directory or LDAP compliant
- **Includes support for Microsoft Active Directory and local user directory on G/On Server**
- **G/On Client connectivity on one IP address or DNS name, multiple IP Ports, and HTTP encapsulation**
- **Includes support for transparent TCP connectivity. Customer must buy one of:**
  - G/On for RDP: Access to office PC and Terminal Server farms
  - G/On for Citrix: Access to Citrix farms
  - G/On for Web Apps: Access to webmail, intranets, portals and other web apps
  - G/On: All of the above
- **Up to twenty menu actions for Client/Server applications connectivity**
- **Field installation of G/On Client and Field Enrollment of user authentication tokens**
- **Dynamic user menus with "Autolaunch" capabilities**
- **Update of G/On Client software and software packages**
- **Logging and Reporting**

# G/On Optional Features & License

## Server Features

- Additional Gateway Servers
- Multiple Client Connect IP Addresses
- LDAP User Directory
- Microsoft SQL Server
- Additional Menu Items
- Login Notification Mail
- Welcome Message
- Wake-on-LAN

## Client Features

- G/On OS

## G/On 5 is Licensed By

- Number of Users (includes 1 token)
  - UAL RDP
  - UAL Citrix
  - UAL WEB
  - UAL
- Number of Tokens (additional)
- Server Features
- Client Features

*Customer or partner receives a mail with signed \*.txt license file with information on licensed features, users and tokens. License file also contains information on maintenance expiration date and – if applicable – a license expiration date.*

*New license file is forwarded when customer acquires additional features, tokens, users, and maintenance.*

# THANK YOU!



[www.giritech.com](http://www.giritech.com)



[www.facebook.com/G.On.Connect](http://www.facebook.com/G.On.Connect)