

G/On™ Short Facts

G/On™ ermöglicht folgende Remote Anbindungen:

- Terminal Server, Microsoft und Citrix
- Remote Desktop Zugriff auf Arbeitsplätze
- ERP- und CRM-Anbindung z. B. SAP, Navision, Microsoft Dynamics, OpenPro
- Access auf Anwendungen, die über TCP/UDP steuerbar sind
- eMail Anbindungen, z. B. Lotus Notes und Microsoft Exchange
- Datenaustausch per FTP
- Anbindung an alle Intranet basierten Systeme, Web-Services und ASP Lösungen

Über Sicherheitszonen können diese Anbindungen wahlweise mit dem auf einem "Trusted PC" vorhandenen G/On™ Desktop Client ausgeführt oder unabhängig und mobil über den G/On™ USB Access Key genutzt werden.

Der G/On™ USB Access Key

Beim G/On™ Access Key handelt es sich um einen speziellen USB-Stick mit einer via G/On™ Server beschreibbaren CD-Partition (nur lesen) und einer Read-Write-Partition. Zusätzlich beinhaltet jeder G/On™ Stick eine weltweit eindeutige Hardware-Seriennummer (EDC), die für die Hardware-Authentifizierung verwendet wird

2-Faktor Authentifizierung mit Single Sign-On

Hierunter versteht man die Kombination aus Hardware- und Benutzer Authentifizierung. Bei G/On™ findet die Hardware-Authentifizierung durch die Freischaltung eines G/On™ USB Access Keys statt (adopt process) oder es wird über den "Trusted PC" eine eindeutige Hardwareseriennummer gebildet, die ebenfalls freigeschaltet werden muss. Erst nach der Authentifizierung erhalten Sie eine Benutzeranmeldung, die wahlweise gegenüber der G/On™ Datenbank oder einem Active Directory Usernamen und Passwort abgleicht. Certificate Server und Token Systeme sind für G/On™ nicht erforderlich, was die Administration erheblich vereinfacht.

Keine Abhängigkeit von Computer oder 3rd Party Produkten

G/On™ bringt einen eigenen Client auf dem USB Access Key mit, der sich auf der CD-Partition des Sticks befindet und unveränderbar ist: Modifikationen durch Malware und unerwünschte AddOns oder ActiveX-Komponenten sind ausgeschlossen. Der erhebliche Vorteil dieses Verfahrens ist die vollständige Unabhängigkeit vom Browser des Computers oder dem dort installierten VPN-Client.

Gleichfalls benötigt G/On™ keine Zusatzkomponenten für das Cache Management oder eine aktive Java Umgebung. Daher kann eine G/On™ Remote-Verbindung zu jeder Zeit mit reinen User-Rechten etabliert werden - ein unschätzbare Sicherheitsvorteil im Vergleich mit den ansonsten notwendigen, lokalen Admin-Rechten zur Einrichtung von Zusatz-, Cache- oder Prüfkomponten bei traditionellen Lösungen.

Lock-to-Process bietet Sicherheit vor unerlaubten Prozessen

Lock-to-Prozess ist eine auf dem von Giritech entwickelten, patentierten EMCADS™ Protokoll basierende Technologie. Grundsätzlich kommuniziert ein G/On™ Client ausschliesslich auf dem lokalen Broadcast 127.0.0.2. Dies hat den Vorteil, dass jeder Angriff von der Client-Seite auf den Client beschränkt bleibt und das dahinter liegende Netzwerk in keinem Fall erreicht. Zusätzlich werden die über G/On™ gestarteten Applikationen über die Prozess ID überwacht.

Vorteile im Überblick

Für den Anwender

- einfachste Handhabung
- unkomplizierter Zugriff
- 2-Faktor Authentifizierung
- kein Browser notwendig
- keine lokale Installation
- überall mobil nutzbar

Für den IT-Admin

- höchste Access-Sicherheit
- zentrales Management
- keine Appliances notwendig
- keine DMZ erforderlich
- ohne Token Server nutzbar
- zusätzliche Firewalls unnötig
- keine Client-Installation
- volle AD-Integration
- kein Mitglied im Netzwerk
- direkter Applikationszugriff
- höchste Verfügbarkeit
- Lastverteilung, voll skalierbar

Typische Einsatzgebiete

G/On™ kommt überall dort zum Einsatz, wo ein schneller, flexibler und kostengünstiger Remote Access auf Business-Applikationen erforderlich ist:

- Aussendienst
- Home Office
- Niederlassungen
- Geschäftspartner
- externe Consultants
- Outsourcing
- Kunden



Diese Prozess ID wird mit der AES 256 verschlüsselten EMCADS Kommunikation fest verkoppelt. Jedem weiteren Prozess erhält eine andere Prozess ID und bekommt damit keinen Kommunikationsweg ins Netzwerk zum Application Server. Malware und unerlaubte Prozesse werden auf diese Weise bereits auf dem Client-Computer (also ausserhalb des Netzwerks und der DMZ) blockiert und können nicht ins Netzwerk kommunizieren - eine effektive Methode, die vor bekannten und unbekanntem Angriffsmethoden schützt.

Wie funktioniert die Kommunikation zum Application Server?

G/On™ ist eine Client/Server Plattform, d. h. der Client auf dem USB Access Key (oder dem "Trusted PC") kommuniziert direkt mit dem G/On™ Server. Dadurch ist der externe Computer zu keinem Zeitpunkt Mitglied des Netzwerks (nodeless client). Er verfügt über keinerlei Zugriff auf allgemein in einem Netzwerk verfügbare Funktionen und Möglichkeiten, wie das Durchsuchen von Server(n) und Freigaben, Identifizieren von IP-Adressen und Namen etc. – was ein erhebliches Plus an Sicherheit darstellt. Der Client kommuniziert ausschliesslich auf der IP 127.0.0.2. Wenn Prozess ID und Authentifizierung korrekt sind, werden die Daten vom "Listener" zum G/On™ Server transportiert. Hier endet die Datenverbindung. Der G/On™ Server baut eine neue Datenverbindung zum jeweiligen Application Server auf und überträgt die Daten.

Das Verhalten ist damit in etwa umgekehrt dem einer traditionellen VPN. Ein Virtual Private Network stellt grundsätzlich eine uneingeschränkte Verbindung her (im eigentlichen Sinne also das genaue Gegenteil von "privat"). Diese wird dann per Firewalls, Intrusion Detection usw. schrittweise abgesichert bzw. reglementiert. G/On™ stellt grundsätzlich weder Kommunikation noch Netzwerkverbindung zur Verfügung. Der Administrator definiert explizit diejenigen Anwendungen, die kommunizieren dürfen - somit sind "versehentlich nicht blockierte Ports" und "unabsichtlich offene Kommunikationswege" definitiv ausgeschlossen.

Einstecken, anmelden - und arbeiten

Zum Remote Access ist praktisch nur der G/On™ USB Access Key erforderlich. Dieser wird automatisch vom G/On™ Server aktualisiert. Er kann im Minimalstfall nur den Client oder den Client plus zusätzliche portable Anwendungen (wie z. B. Navision oder einen portablen, "sicheren" Browser) enthalten. Mit Einstecken des Access Keys wird der Verbindungsaufbau zum festgelegten G/On™ Server initiiert. Es ist keine Installation oder Administration auf der Client-Seite erforderlich. Kollisionen und Konflikte mit bestehenden VPN Clients oder Browser Plugins sind ausgeschlossen.

Vergessen Sie den Cache!

Da der G/On™ Client im "protected monolithic programming" Verfahren entwickelt wurde und ohne Microsoft Memory Manager auskommt, werden am Endpunkt keine verwertbaren Informationen offengelegt, gecached oder in anderer Form hinterlassen. Auch ist es keiner Applikation möglich auf, den Speicher des G/On™ Clients zuzugreifen. Wird allerdings ein auf dem PC vorhandener, lokaler Browser genutzt, dann können Cachedaten auf dem Rechner verbleiben. Deshalb lässt sich der Aufruf auf den USB-Stick umgeleitet, um sichere, definierte Browser wie z. B. Firefox Portable zu verwenden.

Nach Entfernen des G/On™ USB Access Key werden alle über G/On™ bereitgestellten Applikationen sofort geschlossen. Auch auf nicht vertrauenswürdigen PCs bleiben somit keine Spuren oder interne Informationen zurück - selbst dann nicht, wenn der PC neu bootet und die Cache Bereinigung damit nicht mehr greift.

Zentrale Administration

Der G/On Server™ Komponente wird auf einem Windows 2000 oder 2003 Server System installiert. Dort findet auch die zentrale Administration mit (optionaler) Active Directory Synchronisation statt. Die zur Verfügung zu stellenden Applikationen und die Wege, auf denen sie kommunizieren, werden einmalig definiert. Dann werden Sie über Menüs den Usergruppen zugewiesen. Natürlich sind Applikationen auch per "Autolaunch" automatisch startbar.

Die Administration ist vollständig zentralisiert, einfach in der Bedienung, linear und jederzeit nachvollziehbar. Sie beinhaltet bereits konzeptionell immer höchste Sicherheit – gemäss der Giritech Maxime: **Secure by Design.**