White Paper

General Public Use

G/On™

Secure by Design

Deutsche Version 1.0.3

All-in-one Remote Access

Nutzungshinweise und Haftungsausschluss
Die Informationen in diesem Dokument geben ausschliesslich den Kenntnisstand zum Zeitpunkt der Veröffentlichung wieder. Sie wurden sorgfältig recherchiert und zusammengestellt. Wir weisen dennoch ausdrücklich darauf hin, dass die gegeben Informationen aufgrund nicht regelmässiger Aktualisierungen oder Änderungen nicht mehr aktuell sein können. Sämtliche Informationen beinhalten keine Zusicherungen oder Gewährleistungen, auch übernehmen wir keine Haftung für mögliche Schäden, die aufgrund der Nutzung der Informationen entstehen können. Ohne schriftliche Genehmigung dürfen weder Teile dieser Unterlagen noch das Dokument in seiner Gesamtheit für irgendwelche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, auf welche Weise oder mit welchen technischen Mitteln dies geschieht. Bei Unstimmigkeiten, die aufgrund der Übersetzung möglich sind, gelten die Sprachregelungen der englischen Dokumente. Alle genannten Handelsbezeichnungen sind Dienstmarke, Marke oder eingetragene Marke des jeweiligen Inhabers oder Herstellers. Beachten Sie bitte, dass dieses Dokument keine umfassende Beratung durch Giritech oder einen Giritech zertifizierten Partner ersetzt. Aktuelle Produktinformationen, Videopräsentationen, Referenzen und Success Stories finden Sie online unter: www.giritech.de.

Sicherer Remote Access mit G/On

G/On löst alle typischen Sicherheitsanforderungen

Fortschrittliche, integrierte Sicherheitsmechanismen qualifizieren Giritech G/On als strategische Access Plattform für den täglichen Einsatz in (hoch)sensiblen Unternehmensumgebungen. Als "single-vendor" Lösung adressiert G/On alle klassischen Herausforderungen bei der Implementierung von Remote Access Szenarien für interne und externe Anwender.

Die Herausforderungen

Die Auswirkungen des Internets auf unsere Arbeitswelt stellen hohe Anforderungen an die IT-Infrastruktur im Unternehmen, denn das World-Wide-Web wird immer mehr Teil des "lokalen Netzwerks". Während sich durch die Nutzung einerseits Chancen zur Dezentralisierung von Arbeitsplätzen sowie der Neuorganisation von Geschäfts- und Entscheidungsprozessen ergeben, ist andererseits die Absicherung dieser "unkontrollierbaren Wege" von höchster Bedeutung.

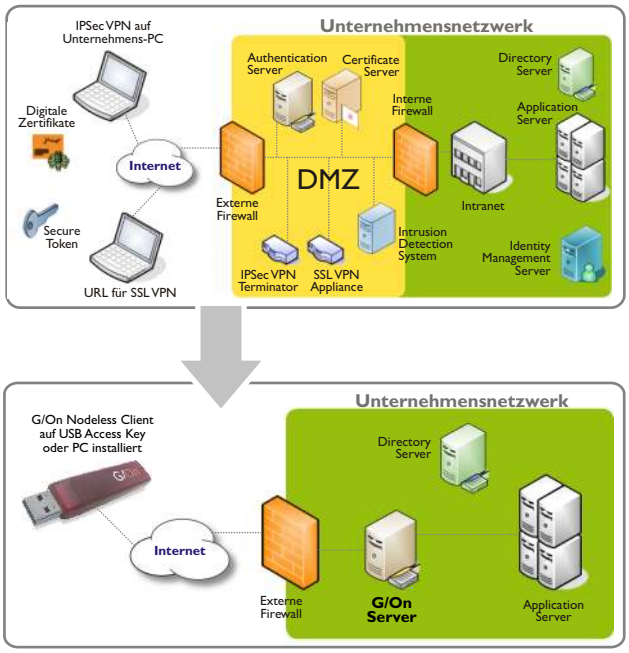
Daher ist es Aufgabe der IT, ein zukunftssicheres, flexibles und kostengünstiges System zu implementieren, das bei geringst möglichem Administrationsaufwand den maximalen (mobilen) Nutzen bietet. Idealerweise lassen sich damit nicht nur die firmeneigenen Mitarbeiter ausstatten sondern auch flexible Zugänge für Berater, Geschäftspartner, Kunden oder Zulieferer auf definierte Ressourcen schaffen.

Secure By Design

Das G/On Produkt ist durch folgende Techniken geschützt:

1. Monolithische Programmierung

Viele bekannte Exploits basieren auf dem Austausch von DLLs durch Trojaner, die zwar scheinbar die korrekte Aktion in Wirklichkeit aber Schadcode ausführen. Monolithische Programmierung bedeutet, dass der gesamte benötigte Code in einer ausführbaren EXE Datei vorhanden ist. Dadurch entfällt die Notwendigkeit, auf externe DLLs für die Basisfunktionalität des Programms zuzugreifen und gleichzeitig muss die Software keine zusätzlichen Maßnahmen (wie z. B. Prüfsummen) ergreifen, um sicher zu stellen, dass externer Code unverändert "echt" ist.



Netzwerkkonsolidierung mit G/On: Von komplexen, traditionell VPN-basierten Strukturen zur transparenten "all-in-one" Lösung mit vereinfachter Administration.

2. Windows Memory Manager

Um das Risiko durch die zahllosen Buffer Overflow Angriffe speziell auf Windows Betriebssysteme zu reduzieren, nutzt die patentierte Client/Server Technologie EMCADS™ (Encrypted Multipurpose Content and Application Deployment System) nicht den Windows Memory Manager. Stattdessen erfolgt die Zuweisung von Speicher für Stack und Buffer durch einen proprietären Speichermanager, der die vollständige Kontrolle über die Speichermanagement-funktionen innerhalb der ausführbaren Datei erhält.

3. Verschlüsselung der ausführbaren Dateien

Alle ausführbaren G/On Dateien sind inklusive DLL und Datendateien in einer Datei verpackt. Die vorhandene EXE ist komprimiert und verschlüsselt, um den Code vor Missbrauch, Reverse Engineering oder Veränderungen in jeglicher Form zu schützen. Die dabei verwendeten Verschlüsselungswerkzeuge bieten einen maximalen Schutz gegen Veränderungen durch Debugging.

Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.

Hochmoderne Verschlüsselung

1. Elliptic Curve Cryptography (ECC)

EMCADS™ verwendet 163-bit ECC für das zeichnende Schlüsselpaar zwischen G/On Server und den G/On USB bzw. G/On Desktop Clients. 163-bit ECC wird ausserdem für den sicheren Schlüsselaustausch und zur Übertragung der Client Identity Facility (CIF) verwendet.

Sobald die Sitzung etabliert ist, werden die ECC Schlüssel zerstört und nicht wieder verwendet.

2. Advanced Encryption Standard (AES)

G/On verschlüsselt den gesamten Datenstrom zwischen Client und G/On-Server mit 256-bit AES (es kommen keine traditionellen VPN-Tunnelingprotokolle wie IPSec, SSL, L2TP and PTPP zum Einsatz). AES stellt eine schnelle symmetrische Verschlüsselung selbst auf langsamen Geräten bereit, die den Datendurchsatz so gut wie nicht beeinträchtigt. Getrennte AES Schlüssel für den Upstream und Downstream der Daten sorgen für erhöhte Sicherheit. Wird eine G/On Session beendet, werden die AES Schlüssel zerstört und nicht wieder verwendet.

Hashing

Nachdem das Datenpaket verschlüsselt ist, kann es in kleinere Segmente von bis zu 1.300 Bytes zerlegt werden. Dies verhindert Paketfragmentierung auf dem Netzwerk-Layer und vermeidet zusätzlichen Overhead.
Die "Zerkleinerung" der Datenpakete erfolgt mittels SHA-1, um Manipulationen während der Übermittlung auszuschliessen.

3. FIPS 140-2 Validierung

Giritechs Kryptografie ist FIPS validiert (Federal Information Processing Standards). FIPS 140-2 ist einer der weltweit führenden und strengsten Sicherheitsstandards, der für international agierende Unternehmen und kommunale Einrichtungen ein wichtiges Entscheidungskriterium bei der Auswahl von IT-Sicherheitslösungen ist.

Integrierte 2-Faktor-Authentifizierung

G/On nutzt eine 2-Wege- und 2-Faktor-Authentifizierung, deren einzelne Komponenten nachfolgend näher erläutert werden.

Die Identitätsdatei (Identity File)

Bei der Installation und Konfiguration eines G/On Servers wird jeweils eine einzigartige Datei erzeugt (Identity File). Diese Datei enhält zur Installation gehörende, eindeutige Informationen, die es dem G/On USB- und G/On Desktop Client ermöglichen, mit dem G/On Server zu verbinden. Die Identity Datei wird während der Erstellung verschlüsselt und kann ohne Sicherheitsrisiko elektronisch an die Clients verteilt werden.

Die initiale Verbindung kommt zu stande, wenn der G/On USB- oder G/On Desktop Client zum ersten Mal gestartet wird. Der Client dekodiert die Identity Datei, um den IP-Namen bzw. die -Adresse des G/On Servers, der kontaktiert werden soll, zu erhalten. Standardmässig erfolgt die Verbindung über Port 3945/TCP (IANA Default für Giritech), es kann jedoch jeder andere, individuelle Port konfiguriert werden. Der G/On Server antwortet mit einer Grussnachricht und der Austausch der sicheren Schlüssel beginnt (Secure Key Exchange - SKE).

Secure Key Exchange (SKE)

Der G/On Server sendet eine Begrüssung mit einem pro-Sitzung öffentlichen ECC Schlüssel sowie einer Signatur. Nur ein G/On Client mit genau der Identity Datei, die auf diesem G/On Server erzeugt worden ist, kann die Signatur des öffentlichen Schlüssels validieren. Dies ist die Grundlage der beidseitigen Authentifizierung und stellt sicher, dass Client und Server für einander konfiguriert sind. Der Client antwortet auf die Anforderung mit der Client Identity Facility (CIF).

Client Identity Facility (CIF)

Die Client Identity Facility (CIF) beinhaltet die EMCADS™ Data Carrier (EDC) Seriennummer. Diese ist entweder die im G/On USB Access Key eingebrannte, eindeutige Seriennummer oder die Seriennummer der Festplatten-Firmware des Computers, auf dem der Desktop Client installiert ist. Die CIF beinhaltet ausserdem eine Anzahl weiterer Identifizierungsmerkmale des Geräts, auf dem G/On ausgeführt wird, wie zum Beispiel:

EDC Serial Number	EDC Firmware	Host OS
Device Volume Label	Public IP Address	OS Major Number
Device Volume Serial	Source Network	OS Minor Number
EDC Manufacturer	Client Hash	Host Class
EDC Media Class	Client Version	Primary MAC Addr.
EDC Interface	Machine Name	
EDC Class	Machine Domain	

All diese Informationen können genutzt werden, um das Gerät während des Adopt-Vorgangs zu identifizieren, den Client in die korrekte globale Zone einzuordnen und dem

Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.

Gerät bei Bedarf spezielle Rollen zuzuweisen. Dies der erste Teil der 2-Faktor-Authentifizierung.

Die CIF enthält auch die gewählte Datenverschlüsselungsmethode, zur Zeit 256-bit AES. Sollten zukünftig leistungsfähigere Verschlüsselungen entwickelt werden, dann sind diese direkt in unsere EMCADS™ Technologie integrierbar.

Globale Zonen

Globale Zonen können, abhängig von der eigenen Sicherheitsdefinition, unterschiedliche Bedeutungen haben: standardmäßig sind sie definiert als „innen, außen und unbekannt". Sie könnten aber ebenso „vertrauenswürdig, eingeschränkt und nicht vertrauenswürdig" heißen. Die grundlegende Idee dieses Konzepts ist, dass abhängig vom geographischen Aufenthaltsort des Anwenders sowie des verwendeten Geräts, bestimmte Applikationen freigegeben oder gar nicht erst nicht verfügbar gemacht werden.

Regeln

Die in G/On nutzbaren Regeln ermöglichen das Verbieten eines Geräts, die Ablehnung eines Geräts sowie die Zuordnen eines Geräts in eine Zone, basierend auf den bekannten Informationen über das Gerät aus der CIF.

Login Dialog

Der zweite Bestandteil der 2-Faktor-Authentifizierung ist der Anmeldefenster. Sobald das Gerät, auf dem sich der Client befindet authentifiziert ist, muss der Anwender seine Benutzerkennung (User-ID) sowie sein Passwort eingeben.

Dabei können folgende Möglichkeiten gelten:

- der G/On Client kann nur von einem dedizierten User verwendet verwenden
- der User darf nur einen zugewiesenen Client verwenden
- die Kombination aus User und Client (USB Access Key) ist fest hinterlegt und funktioniert nur in dieser Kombination.

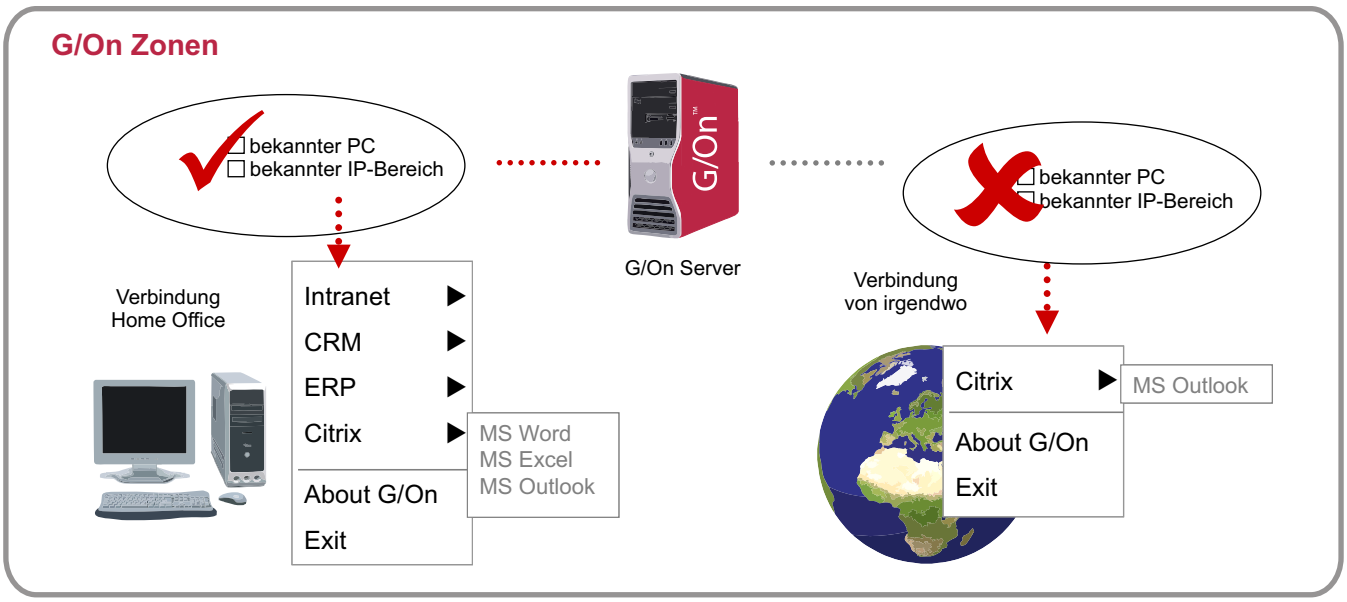
Der Login-Dialog selbst ist mit verschiedenen Funktionen ausgestattet, um sogenannte brute-force Angriffe zu verhindern:

- fehlgeschlagene Logins
- Login-Fenster an einer zufälligen Position des Bildschirms anzeigen
- verhindern der Navigation per TAB Taste
- wechseln der Funktionsweise von "OK" und "Cancel"
- Nutzung des On-Screen-Keyboards (OSK) zur Eingabe
- OSK automatisch aufrufen
- Verbindungsabbruch, sobald der Bildschirmschoner aktiv wird

Eine sinnvolle Kombination der Möglichkeiten basiert sowohl auf den internen Sicherheitsrichtlinien als auch dem "Gefahrenpotenzial" der Umgebung, in der G/On eingesetzt wird.

Umfassender Schutz vor Malware

Da die G/On nicht netzwerk- sondern anwendungsbasiert arbeitet, ist aufgrund der fehlenden IP-Konnektivität eine Kompromittierung des LAN/WANs durch Viren, Würmer, Spyware, man-in-the-middle Angriffe oder sonstige Malware ausgeschlossen.



Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.

Das Loopback Interface und Split-DNS
Die Verbindung zwischen dem G/On Server und dem G/On Desktop- oder USB-Client über Port 3945/tcp ist auf das Loopback Device des Clients gebunden - genauer gesagt auf 127.0.0.2. Das Socket Gateway (das Teil des G/On Clients ist), öffnet einen Socket für den verwendeten Port, z. B. 127.0.0.2:80 für http Traffic. Nun werden alle Daten, die an einen eingerichteten Socket auf 127.0.0.2 gesendet werden, verschlüsselt und durch den Port 3945/tcp an den Server geschickt.

Split DNS wird verwendet, wenn der Server einen Redirect von 127.0.0.2 auf einen tatsächlichen Hostnamen sendet. Dies bedeutet, dass nach innen der Hostname in die korrekte IP-Adresse aufgelöst wird, nach außen jedoch 127.0.0.2 bestehen bleibt. Idealer Nebeneffekt: Jeder Hacking-, Viren- oder Backdoor-Angriff und Scanning-versuch findet auf dem PC des Hackers selbst statt, nämlich auf seinem Loopback Interface, da alle IP-Adressen der zu attackierenden Server in 127.0.0.2 auf der externen DNS aufgelöst werden.

Man-in-the-Middle Attacken
Alle Daten, die durch eine G/On Verbindung gesendet werden, enthalten eine Prüfsumme und einen SHA-1 Hash. Wenn diese nach dem Empfang der Daten an einem der beiden Enden nicht korrekt sind, wird die Verbindung beendet. Dies schützt effektiv vor Man-in-the-Middle Angriffen.

Da G/On niemals einen identischen Satz von ECC oder AES Schlüsseln zweimal verwendet, sind Replay-Attacken praktisch ausgeschlossen. Ein G/On Client kann vielleicht auf das erste Paket einer Simulation durch einen Replay-Server reagieren, aber der Replay-Server wird niemals in der Lage sein, die Antwort eines zulässigen G/On Clients zu entschlüsseln. Ebenso gelingt es einem Replay-Client niemals einem G/On Server zu antworten, da unbekannt ist, was in ein Datenpaket eingebunden werden muss, um die Anforderungen der G/On “Regeln- und Zonen-Engine” zu erfüllen.

Viren, Spyware, Trojaner usw.
G/On arbeiten applikations- und nicht netzwerkbasiert, deshalb ist es für viele Arten von Viren, Spyware oder Trojanern nicht möglich, das Unternehmensnetzwerk zu beeinträchtigen. Natürlich bedeutet dies nicht, dass G/On selbst sicher vor Viren, Spyware, Trojanern oder Backdoor-Angriffen ist sondern dass es G/On diese Angreifern extrem schwierig macht, sich in das Netzwerk auszubreiten.

Mit der richtige Konfiguration von G/On und den über G/On konnektieren Anwendungen, kann tatsächlich dafür gesorgt werden, dass Infektionen der im Unternehmensnetzwerk zur Verfügung gestellten Services praktisch ausgeschlossen sind.

Und obwohl die Sicherheit des Endpunkts für die reine G/On-Verbindung keine entscheidende Rolle spielt, sollte der PC natürlich im eigenen Interesse mit Firewall, Anti-virus- und Antispyware-Software geschützt werden.

Phishing Angriffe
Phising kann effektiv eliminiert werden, wenn Anwender konsequent nur über G/On zugreifen und lernen, niemals verdächtige E-Mail Links zu aktivieren.

Da die Verbindung auf Anwendungen durch das Loopback Interface des Client-PCs fliesst, haben Versuche die URL zu ändern keine Auswirkung, da der Client immer auf 127.0.0.2 verbindet und die vollständige URL nur auf der G/On-Serverseite bekannt ist.

Fakten: G/On und Keylogger / Spyware

Durch die integrierbare Kombination aller hier genannten Features in Verbindung mit der 2-Faktor-Authentifizierung geht G/On deutlich über die Standardsicherheit traditioneller VPNs hinaus. Die Einbindung der entsprechenden Security-Prozesse in die G/On Umgebung wird abhängig von den Sicherheitsanforderungen in Zusammenarbeit zwischen Anwender und Giritech bzw. einem durch Giritech autorisierten Partner realisiert.

Grundsätzlich gilt aber auch für G/On wie für jede andere Anwendung, dass ein Sicherheitsverständnis beim Anwender vorhanden sein muss und sich dieser an die Security Policy des Unternehmens hält.

Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.

Lock To Process Applikationskontrolle
"Lock To Process" definiert die Fähigkeit, dass nur Anwendungen, die vom G/On Menü aus gestartet worden sind, ihre Daten durch das Loopback Interface senden dürfen. Wird eine Anwendung (z. B. ein Webbrowser) gestartet, dann enthält die Konfiguration Informationen darüber, welchen Port und welches Protokoll die Anwendung nutzt. G/On öffnet auf dem Loopback Interface einen Socket, der auf den richtigen Port hört - im Beispiel des Webbrowsers könnte dies TCP Port 80 auf der IP-Adresse 127.0.0.2 (127.0.0.2:80) sein. Die Prozess-ID des Webbrowsers wird dann auf den Socket gebunden und nur diese Prozess-ID kann dann Daten an diesen Socket senden. Versucht eine andere Anwendung, wie ein Virus oder Trojaner, Daten zu senden, dann werden diese durch G/On einfach ignoriert.

Applikations- versus Netzwerkzugriff

G/On bietet im bisher von IPSec- und SSL-VPN dominierten Connectivity-Markt eine unkomplizierte und sichere Methode, um Anwender via Internet oder im LAN mit Applikationen virtuell zu verbinden.

Die Kombination aus Hard- und Software unterscheidet sich von klassischen VPNs technisch dadurch, dass G/On keine direkte Verbindung in das Netzwerk etabliert sondern nur authentifizierte User auf spezifische Applikationsserver verbindet.

Network to Network Connectivity
Für IT-Abteilungen ist es heute reine Routine, zwei Netzwerkwerke mit identischer Technologie und den selben Sicherheitsrichtlinien innerhalb des Unternehmens zu verbinden. Diese "Netzwerk-zu-Netzwerk" Konnektivität ist ein üblicher Weg, um Niederlassungen mit Anwendungen und Daten der Hauptstelle zu versorgen.
Die Herausforderungen beginnen dann, wenn ein unabhängiges Netz - z. B. eines Partners, Zulieferers oder Kunden - an die eigene Infrastruktur angebunden werden muss. Oftmals unterscheiden sich nicht nur Security Policies und Ausstattung voneinander sondern auch die Art und Weise, wie die IT generell gehandhabt wird. Im Ergebnis sind solche Prozesse mühselig und führen nicht selten zu einer reduzierten Funktionalität im Hinblick auf die eigentlich angestrebte Nutzung.

Application Connectivity
Anwendungskonnektivität repräsentiert einen neuen Weg, um Partner, Kunde, Berater und jede andere Instanz miteinander zu verbinden. Die Notwendigkeit einer Netzwerk-zu-Netzwerk Verbindung wird eliminiert, da der Client-Computer mit einem Server kommuniziert - und dieser Server die Konnektivität zu den Applikations-systemen bereitstellt. G/On ist eine solche Client/Server Lösung: Der G/On Server wird einfach im internen Netzwerk plaziert und eliminiert die zusätzlichen Kosten für VPN/SSL-VPN, Token, Zertifikate und alle sonstigen Technologien, die typischerweise eingesetzt werden, um Remote Access anbieten zu können.

Da der Client-PC niemals zum Bestandteil des internen Netzwerks wird, ist die Wahrscheinlichkeit einer Vireninfektion oder der Verbreitung von Trojanern, Spyware usw. praktisch gleich Null. Außerdem besitzt G/On keine Broadcast-Adresse: Der Server ist nur „Zuhörer" und antwortet ausschließlich auf autorisierte Datenströme. Im Gegensatz zu SSL VPNs werden auch keine Daten lokal gecached oder zurückgelassen, die ein möglicher Angreifer ausnutzen könnte. Ohne USB Access Key ist nicht einmal eine Adresse bekannt, über die ein potenzieller Hacker den Server finden und versuchen könnte, die Verbindung erneut aufzubauen.

Gleichzeitig reduziert G/On die Anzahl der offenen Ports, die zur Kommunikation notwendig sind, auf eine einzigen TCP Port (standardmässig 3945/tcp, aber frei änderbar). Dies erhöht die Sicherheit und reduziert effektiv den Traffic im Netzwerk (keine Broadcasts und Pakete mehr durch an das LAN angeschlossene Systeme).

In Verbindung mit den G/On Zonen, der Gruppen-zuordnungen im AD sowie der UserID ist die Freigabe von Anwendungen exakt vom Vertrauensgrad in das verwendete Endgerät sowie die geografische Position des Users abhängig.

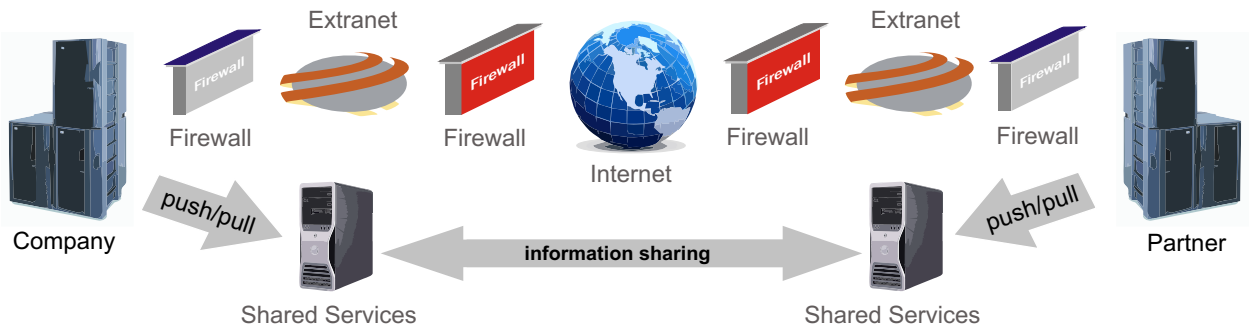
Vorteile einer Application Connectivity

- keine Offenlegung des Netzwerks nach außen
- Security Policies müssen nicht vereinbart werden (die firmeneigenen Richtlinien werden immer durchgesetzt)
- Inkompatibilitäten zwischen Geräten und Strukturen werden eliminiert
- Implementierungs- und Administrationskosten sind vergleichsweise gering
- das Unternehmen wird zum Service-Provider und bietet die Dienstleistung "Remote Access" für Mitarbeiter, Kunden und Partner an

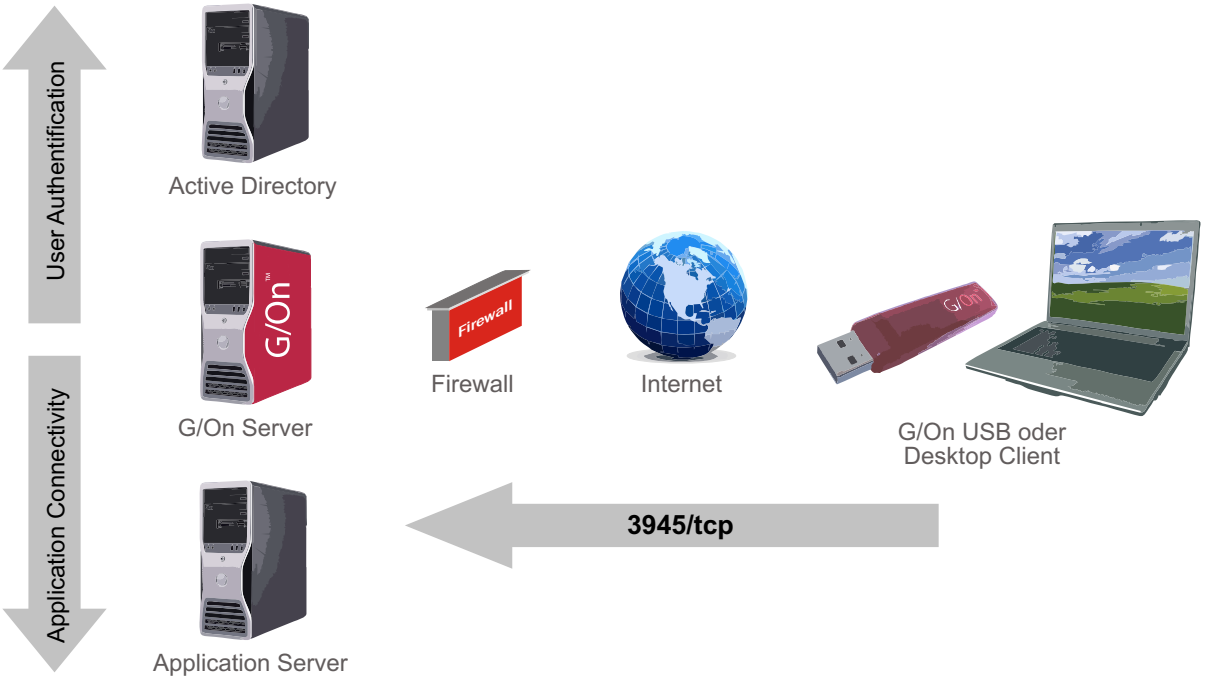
Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.

Typische “Network to Network” Connectivity



Application Connectivity mit G/On



Weitere Informationen zur Serverplazierung finden Sie im “Best Practice Reference Guide” sowie im “G/On Admin Guide”. Beider Informationen erhalten Sie auf Anfrage über Giritech.

Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech’s core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.

EMCADS™

Encrypted Multipurpose Content and Application Deployment System

Der EMCADS Serverkern ist eine Transaktionsengine, die entwickelt worden ist, um Analyse- und Verarbeitungsverfahren der patentierten “dynamic datagram” Methoden zu unterstützen.
Der Serverkern implementiert ein hochmodulares Design, das maximale Flexibilität für künftige Erweiterungen der Grundfunktionen unterstützt. Nahezu jeder Teil des Codes oder der Funktionen können mit geringstem Entwicklungsaufwand ersetzt werden - dies betrifft selbst die CRC- und Datenverschlüsselungs-Engines.

Grundsätzlich kann der EMCADS Server als eine Art Proxy-Server betrachtet werden, da er alle Aufgaben für die User erledigt und es niemals eine direkte Kommunikation zwischen Anwender (oder verbundenem Client) und irgend einem Server oder einer im Netzwerk erreichbaren Ressource gibt. Alle Anfragen werden innerhalb des EMCAD Servers analyisiert und dann im Auftrag des Users bei dem Zielsystem angefragt.

Die von EMCADS verwendete Datenverabeitungsmethode ist deshalb so effizient, weil es aufgrund der dynamischen Struktur so gut wie nie redundante Daten oder Lücken gibt: Die Datenpakete werden nicht nur zur selben Zeit geprüft und verarbeitet (was wertvolle Berechnungszeit spart), auch die Menge der über das Netzwerk zu übertragenden Bytes wird durch EMCADS reduziert.

1. EMCADS™ Clients
Der Basisclient stellt keine hohen Speicheranforderungen und sorgt dafür, dass Anwender schnell und einfach von jedem Internet-basierten Gerät aus mit dem EMCADS Server verbinden können.
Die grafische Oberfläche und alle verfügbaren Funktionen werden vom Systemadministrator nach den spezifischen Anforderungen der User definiert. Der G/On Client kann mit nahezu jedem personalisierten Speichermedien ausgerollt werden, wie beispielsweise G/On USB Access Key, CD-ROMs, SIM-Karten, SD-Karten oder SmartCards. Auf diese Weise werden “dumme” Speichergeräte in sogenannte EMCADS™ Data Carriers (EDCs) verwandelt. Um die Nutzung bestimmter Netzwerkressourcen zu vereinfachen, ist oft ein zusätzlicher Client von Drittanbietern auf dem EDC enthalten, beispielsweise ein Citrix ICA Client oder ein Terminal Services RDP Client.

2. Der EMCADS™ Server
Im EMCADS Serverkern liegt ein Datenprüfungs- und -verarbeitungsmechanismus, der die patentierte “Dynamic Datagram Parsing Engine” einschliesst. Das Design des Kerns zeichnet sich durch eine vollständig ereignisgetriebene, transaktionsorientierte Verarbeitungsengine aus. Sie analysiert die dynamischen Datenpakete und bietet eine Reihe von Vorteilen:

• Jede Anwendersitzung verfügt über eine eigene Transaktionswarteschlange. Dadurch kann der Server aktiven Anwendern mehr Zeit einräumen als inaktiven Usern und so im Bezug auf die Zuteilung von Ressourcen mit maximaler Effizienz arbeiten.

• Die Datenpakete sind hochdynamisch, denn jedes Paket enthält immer nur die Header, die für den jeweiligen Zweck gerade erforderlich sind. Die Präsenz und/oder der Inhalt eines Header-Felds sowie die Richtung des Datenpakets definiert das Vorhandensein oder das Ausbleiben des nächsten Header-Felds.

• Nahezu jede heute verfügbare Verschlüsselungsmethode kann unterstützt werden - und eine Anpassung an zukünftige Verschlüsselungsstandards ist sehr einfach realisierbar.

• Die Validierung des Zugriffs erfolgt auf zwei Wegen: Zuerst wird das aktuell verwendete Gerät gegenüber den Regeln validiert, um festzustellen, ob es erlaubt ist oder nicht. Im zweiten Schritt muß sich der Anwender identifizieren und validieren. Da alle Zugriffsregeln vollständig am G/On Server durch den Administrator kontrolliert werden, kann praktisch jede Sicherheitsregel durchgesetzt werden . So erhalten nur die Anwender einen Zugriff, die mit dem passenden Profil verbunden sind.

Grundlegende Funktionsweise

Eine Standardsitzung mit G/On durchläuft 4 Phasen:

- Verbindung
- Authentifizierung (Rechte und Policies)
- Ressourcenzugriff
- Beenden der Verbindung

Im Folgenden betrachten wir diese gesondert.

Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.

Verbindung

1. Der EMCADS™ Client versucht automatisch mit dem EMCADS™ Server zu verbinden. Der EMCADS™ Server erzeugt eine zufälliges öffentliches/privates 163-bit ECC Schlüsselpaar, signiert den öffentlichen Key und sendet ihn zusammen mit der Signatur an den Client.

2. Der Client validiert die Signatur auf dem öffentlichen Schlüssel gegenüber den vorab verteilten Zertifikaten. Schlägt die Validierung des Zertifikats fehl, dann beendet der Client die Verbindung ohne weitere Aktivität.

3. Ist die Validierung der Signatur am Client erfolgreich, dann erstellt der Client im Gegenzug ein gleiches öffentliches/privates 163-bit ECC Schlüsselpaar. Danach stellt der Client ein "Client Identity and Facility Package" (CIF) zusammen. Dieses enthält unter anderem eine Liste unterstützter Verschlüsselungsverfahren, Hashes (zur CRC Prüfung), Bitlängen, den symetrischen Schlüssel für den Upstream und zusätzliche Informationen über das Gerät, auf dem der Client läuft inklusive der Seriennummern für die Giritech G/On USB Access Keys.

4. Diese Informationen werden mit dem öffentlichen Schlüssel des Servers codiert und zurück gesendet.

5. Der Server entschlüsselt und validiert das Paket (sowie das Zertifikat, falls verwendet). Schlägt die Validierung fehl, dann beendet der Server die Verbindung.

6. Ist die Validierung erfolgreich, wird im nächsten Schritt die Client-ID, die USB-KEY ID oder weitere Informationen, die durch den Client übermittelt worden sind, gegenüber den Regeln überprüft, die der Administrator auf dem Server vorgegeben hat. Basierend hierauf entscheidet der Server, ob er auf die Anfrage antwortet oder sie ablehnt.

7. Besteht der Client die Überprüfung der für einen Zugriff definierten Regeln nicht, dann beendet der Server die Verbindung zum Client sofort.

8. Ist die Prüfung des Clients erfolgreich, dann prüft der G/On Server, welche der verfügbaren Verschlüsselungsverfahren für die Sitzung verwendet werden kann. Der Server wählt grundsätzlich die stärkste der verfügbaren Verschlüsselungen. Außerdem erzeugt der Server einen zufälligen symetrischen Schlüssel für den Downstream, verschlüsselt alles mit dem öffentlichen Schlüssel des Clients und gibt diese Daten weiter.

9. Der Client erhält diese und wechselt auf das symetrische Verschlüsselungsverfahren. Danach tauschen Client und Server "Quittungen" aus, um sicherzustellen, dass die symetrischen Systeme funktionsfähig sind.

Standardmässig verwendet EMCADS™ eine 256-bit AES Verschlüsselung, der Server kann jedoch nahezu jedes andere symetrische Verschlüsselungsverfahren unterstützen und so konfiguriert werden, dass er multiple Schlüssellängen, Schemata, Rückmeldungen usw. unterstützt und sogar unterschiedliche Codierungen, Schlüssel und Prüfsummen für Up- und Downstream bei bestimmten Anwendungen unterstützt.

Das "Content-Paket" ist ein proprietäres Format, in dem der gesamte Inhalt des Pakets (der sowohl aus Befehlen für den Server als auch tatsächlichem Inhalt bestehen kann), verschlüsselt wird. Für den Datentransport wird das zugrund liegende TCP/IP verwendet, allerdings verläßt sich das EMCADS™ Protokoll auf keinerlei Informationen oder Header des TCP oder IP Protokolls. Dadurch ist es voll transparent gegenüber jeder Art von NAT, PAD oder zusätzlichem Tunneling bzw. weiteren Verschlüsselungen.

Will der Client mit dem Server kommunzieren, füllt er die Header-Felder aus, fügt optional die Nutzdaten an und übergibt dies an die eingebettete EMCADS™ Client Data Management Engine. Diese verschlüsselt das gesamte Datenpaket mit dem für die Sitzung gewählten Codierungsverfahren und sendet das Paket an den Server. Sobald der EMCADS™ Server das Paket erhält, wird es entschlüsselt und validiert, um festzustellen, ob es auf der Transportstrecke verändert worden ist. Danach verarbeitet der G/On Server den Header sowie die optionalen Nutzdaten und führt die notwendigen Aktionen aus.
Falls das Paket an einen anderen Nutzer oder zum Beispiel einen anderen EMCADS™ Server weitergeleitet werden muss, wird es basierend auf der aktuellen Sitzung erneut verschlüsselt.

Authentifizierung

Derzeit unterstützt EMCADS™ das "Microsoft Active Directory (AD)" über die Windows-eigene API sowie eine G/On-eigene Authentifizierung. Andere Verfahren, wie zum Beispiel RADIUS, TACACS, Cisco AAA und biometrische Verschlüsselungen, können durch Giritech optional auf Anforderung implementiert werden.

Sobald die Verbindung etabliert ist, erscheint ein Standard-Dialogfenster, in dem der Anwender seinen Benutzernamen sowie das Passwort eingibt. Ist die Authentifizierung erfolgreich, registriert der EMCADS™ Server den Client sofort als "online" im lokalen User-Verzeichnis.

Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.

Der EMCADS™ Client unterstützt auch zusätzliche Methoden für eine automatisierte Anmeldung (wie “single Sign-on”), die primär dann verwendet werden, wenn der Client selbst oder andere Giritech Clients (z. B. der GRDP-Client oder TClient) eine Sitzung etablieren müssen. Am häufigsten verbreitet ist eine Anmeldung über zufällig generierte Einmaltoken.

Ressourcennutzung
Anwender können, sobald sie mit dem System verbunden sind, nur auf diejenigen Netzwerkressourcen zugreifen, für die sie autorisiert sind. Dies bedeutet, sie können die Server, Dateien und Peripheriegeräte sehen, für die sie gemäß der Gruppen- bzw. Namenszugehörigkeit berechtigt sind - aber alles andere im Netzwerk ist nicht sichtbar.

Dies ist ein wichtiger Unterschied beispielsweise gegenüber IPSec VPNs, die eine Verbindung auf der physikalischen Netzwerkebene herstellen und bei denen weitergehende Filterungen eine zusätzliche Firewall voraussetzen. Auch unterscheidet sich G/On in diesem Punkt von traditionellen SSL VPNs, die ausschliesslich web-basierten Zugriff ermöglichen, sprich: Sie benötigen bei SSL-VPNs ein Web-Interface, um überhaupt arbeiten zu können und alle im Cache befindliche Informationen müssen nach der Sitzung wieder entfernt werden.

EMCADS™ unterstützt neben dem fein abgestuften Rechtemanagement und der Möglichkeit, Befehle einzubetten auch Sitzungen, die ständig aktiv sein können.

Verbindungstrennung
Um die Verbindung zu trennen, kann der Anwender entweder den “Exit” Befehl im G/On Menü nutzen oder einfach nur den G/On USB Access Key am Computer abziehen. Der Client erkennt, dass der USB Key entfernt worden ist, trennt sofort die Verbindung zu den Servern und beendet sich.

Der G/On USB Client nutzt ausschliesslich die Internet-Verbindung sowie den Hauptspeicher des Computers - es wird weder Software auf die Festplatte geladen noch werden die Ressourcen des Geräts in anderer Weise genutzt (u. a. keine Nutzung der Registrierungsdatenbank, kein lokales Caching, keine Verwendung des Microsoft Speichermanagers). Dies bedeutet, dass keinerlei verwertbare Informationen der Session auf dem Computer zurückbleiben, die dazu genutzt werden könnten, um das G/On System, die Verbindung oder das Unternehmens-netzwerk zu kompromittieren.

Technische Vorteile der Lösung

Sicherheit
EMCADS™ kombiniert höchste Sicherheit mit maximaler Flexibilität für die Anwender, die remote in beliebiger Weise auf Netzwerkressourcen zugreifen möchten. Die Vorteile sind:

- starke 2-Faktor-Authentifizierung
- nodeless client (Client ist nicht Mitglied im LAN)
- starke, selbst-modifizierende Verschlüsselung des gesamten Datenstroms
- der Server antwortet nur authentifizierten Clients auf genau 1 Port
- vollständige Kontrolle über die Nutzung aller Netzwerkressourcen
- völlige Transparenz und Nachweisbarkeit aller Aspekte der Remoteverbindungen

Theoretisch wäre es für einen Angreifer möglich, einen eigenen Client anzufertigen - dieser würde jedoch niemals einen Zugriff auf das System erhalten. Denn der Angreifer müßte durch “brute force” Techniken den Private Key Bereich des Servers und die per Sitzung zufällig generierten, temporären ECC Schlüsselpaare des Clients erhalten, um an Informationen über die zufällig erstellten Keys, die involvierten Prüfsummen und jeden Feedback-Algorithmus oder andere selbstverändernde Mechanismen in G/On zu erhalten. Legt man das Niveau der verwendeten Verschlüsselung zu Grunde, sowie die Tatsache, dass alle Codierungsschlüssel zufällig, pro Sitzung generiert und für Up- und Downstream unterschiedlich sind, dann ist ein solcher Angriff technisch nicht möglich.

Außerdem würde spätestens in dem Moment, in dem ein “echter” Client Daten an den Server sendet (mindestens einmal pro Minute) sowohl die Session des gefälschten als auch des “echten” Clients sofort durch den Server terminiert werden, denn dieser erkennt den Versuch, Daten in den verschlüsselten Strom einzuschleusen.

Falls ein Client Gerät verloren oder entwendet wurde, kann es sofort am G/On Server deaktiviert werden. Alternativ läßt sich das System so konfigurieren, dass jeder weitere Nutzungsversuch mit einer entsprechenden Meldung (z. B. Bitte um Rückgabe des Keys) quittiert wird. Optional kann der nicht authorisierte User zugelassen und in einen “Quarantäne”-Bereich umgeleitet werden (”Honeypot”), in dem das System versucht, den physikalischen Ort des Keys aufgrund der aktuellen Host-Daten zu lokalisieren.

Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech’s core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.

Die Tatsache, dass EMCADS™ ausschliesslich eine virtuelle Applikationsverbindung aufbaut (im Gegensatz zu einer physikalischen Netzwerkverbindung bei VPNs) limitiert den für jeden User verfügbaren Grad an Interaktion und Zugriff. Außerdem läßt sich jeder Verbindungsaspekt präzise beobachten und registrieren, da alle Anfragen über EMCADS™ abgewickelt werden.

Übrigens ist jede Giritech Software, EMCADS™ Server wie Clients, nicht nur verschlüsselt sondern auch gegen Modifikationen von außen geschützt (wie z. B. Debugger, Disassembler, Tracer, Code- und API-Hooking Tools, Werkzeuge zum Auslesen bzw. Verändern des Speichers, Entry-Point-Modification und mehr). Hacker, Viren oder Trojaner können aus diesem Grund die G/On Lösung nicht kompromittieren.

Mobilität

Der Formfaktor des USB Access Keys sowie die hohe Kompatibilität zu verschiedenen Host-Systemen bedeutet für die Anwender maximale Mobilität. Standardmässig genügt ein Computer mit USB-Anschluss, eine aktive Internet-Verbindung sowie eine Firewall, die Outbound-Traffic zulässt, um von überall aus zugreifen zu können. Somit können G/On User unterwegs auch ohne eigenen Laptop hochsicher auf die Ressourcen des Unternehmens zugreifen.

Einfache Bedienung

G/On ist für Anwender äußerst einfach zu bedienen, denn sie benötigen lediglich ihren Benutzernamen und ihr Passwort, um die Verbindung aufzubauen. Viele komplexe Sicherheitssysteme verwirren und irritieren den durchschnittlichen Anwender so häufig, dass Systeme letztlich nicht oder nur ungern genutzt werden - bzw. der User einen Weg sucht, um die Mechanismen zu umgehen. Bei G/On hingegen muss der Anwender weder Profi sein, noch vorkonfigurierte Laptops benutzen oder sich komplizierte Vorgehensweisen merken.

2-Wege-Echtzeitkommunikation

EMCADS™ ist so performant, dass auch zeitsensible Anwendungen wie IP-Telefonie (VoIP) oder Videokonferenzen (AvoIP) nutzbar sind. Dies ist ideal für eine breitbandige Nutzung portabler und stationärer internetfähiger Geräte, die Echtzeitkommunikation unterstützen.

Single Point of Entry

EMCADS™ bietet einen zentralen Zugangspunkt für Mitarbeiter, Partner, Kunden, Berater und andere Personen, die mobilen Access benötigten. G/On kennt die Identität jedes Users, der für den Zugriff auf das Netzwerk autorisiert ist. Die Lokation des Netzwerks wird nicht bekannt gegeben, da der EMCADS™ Server keinen Broadcast ausführt. Er antwortet nur auf Verbindungsanfragen von Clients, bei denen die erste Authentifizierung erfolgreich war. Dies maximiert die Sicherheit, minimiert den Wartungsaufwand und ist gegenüber traditionellen Lösungen deutlich kosteneffizienter.

Zentralisierte Kontrolle

EMCADS™ protokolliert jedes Detail jeder Verbindung zwischen Client und Server. Dadurch ist die Protokollierung, Verfolgung und Überwachung aller Daten, die in ein Netzwerk eintreten, es verlassen oder darin transportiert werden, einfach und kostengünstig realisierbar. Organisationen haben somit die Möglichkeit, präzise zu dokumentieren, was welcher Anwender im System tut. Dies minimiert den Bedarf an Intrusion Detection Systemen (IDS) oder anderen Netzwerküberwachungsverfahren.

1. Authentifizieren der User	2. Absichern von Geräten	3. Schützen der Daten	4. Filtern des Netzwerkzugangs	5. Kontrollieren und verwalten
				☑ MS Outlook ☑ Navision ☒ SAP Client ☒ Terminal Server ☑ Remote Desktop ☑ CRM Datenbank ☒ PCs
Starke, wechselseitige 2-Faktor-Authentifizierung, eindeutiger Access-Key, Device ID + Passwort	Virtuelle Applikationsverbindung, lock-to-process, PC ist nicht Teil des Netzwerks	Hochgeschwindigkeits-verschlüsselung mit 256 Bit AES und Prüfsummen	"Lautloser" Server, der nur G/On™ authentifizierten Clients antwortet	Direkte Verbindung auf spezifische Applikationen

G/On löst alle 5 Herausforderungen für sicheren und mobilen Remote Access

Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.

Flexibilität und Rollout

EMCADS™ ist eine sogenannte “core” or “deep infrastructure” Technologie, die breitbandig an eine Vielzahl existierender Tolopogien, Systeme und Anwendungen angedockt werden kann - mit sehr geringen Veränderungen oder direkt “aus der Box”. Der größte Teil der Technologie basiert auf offenen Standards und aufgrund des modularen Designs ist G/On einfach auf individuelle Anforderungen anpassbar. Sowohl die Funktionen als auch das Interface für die Anwender läßt sich sehr leicht erweitern und mit geringem Aufwand verändern. Im Vergleich mit anderen IT-Sicherheitslösungen läßt sich eine G/On Lösung im Bruchteil der Zeit vorbereiten, installieren und ausrollen.

Geeignet für Enterprise-Umgebungen

G/On läßt sich schnell, einfach und kosteneffizient skalieren, um die Access-Anforderungen von Unternehmen jeder Größe zu erfüllen - von KMU/SoHo- bis Enterprise-Umgebungen. Fügen Sie einfach weitere Server oder optionale Module hinzu. Die G/On Technologie unterstützt load-sharing Szenarien und fail-safe Redundanz, so dass auch unternehmenskritische Anwendungen problemlos in das Konzept integriert werden können.

Weiterführende Links

http://de.wikipedia.org/wiki/Elliptic_Curve_Cryptography
http://en.wikipedia.org/wiki/AES
http://en.wikipedia.org/wiki/SHA-1
http://www.giritech.de/giritech-gon-fips140-2.htm

Die wichtigsten Sicherheitsfeatures auf einen Blick:

- G/On bietet eine leistungsstarke 2-Faktor-Authentifizierung und ist FIPS 140-2 validiert.
- Weder das Kopieren des Software Clients, noch der Dateien des USB-Access-Keys auf Drittsysteme ermöglichen einen Zugriff auf das System. Der Client kann nicht oder nachgebildet modifiziert werden.
- G/On verwendet zur Verschlüsselung 256 Bit AES und 163 Bit starke ECC Schlüssel.
- Ohne Authentifizierung des Clients am G/On Server sind keinerlei Aktivitäten ausführbar (Client besitzt keine „Intelligenz” und keine Informationen über Menüs oder Server).
- Wechselseitige Authentifizierung (sowohl client- als auch serverseitig) zur Vermeidung von Phishing/Pharming Angriffen.
- G/On realisiert ausschliesslich Applikations-anbindungen, KEINE Netzwerkanbindung.
- Alle bereitgestellten Applikationen werden zentral administriert. Auch das Deployment neuer Software kann zentral über den G/On Server (remote) durchgeführt werden.

Aufbau einer Remote Access Verbindung mit G/On

Schritt 1
Der G/On™ Access Key wird einfach in einen aktiven USB-Port eines internetfähigen PCs eingesteckt. Der G/On™ Client startet dann automatisch. Alternativ kann die kostenlose Desktop-Software auf einen PC kopiert und an Ihrem G/On™ Server eindeutig aktiviert werden (adopt). USB Key oder PC sind Bestandteil der integrierten 2-Faktor-Authentifizierung.

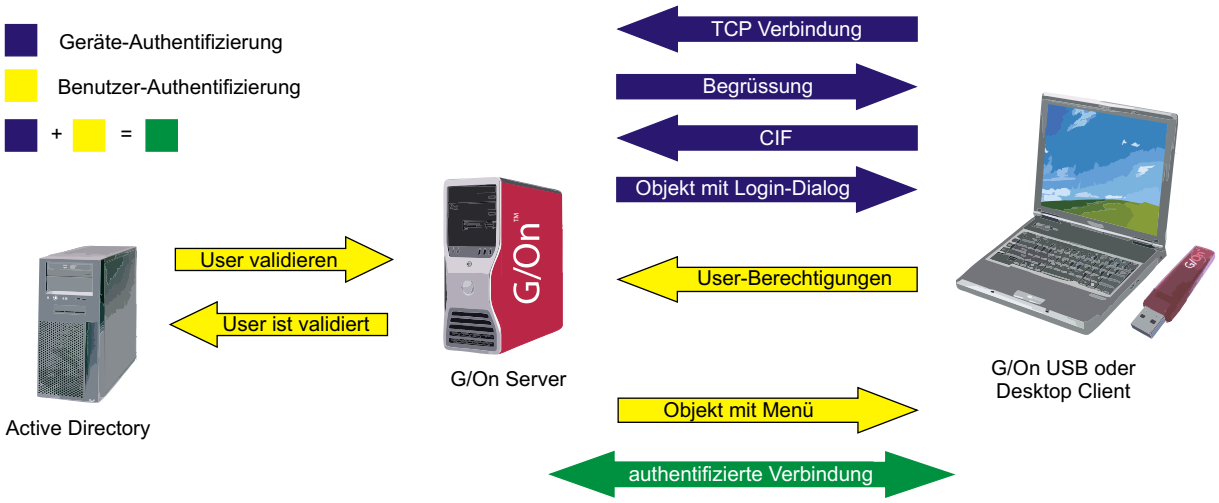
Schritt 2
Im Login-Dialog autorisieren Sie sich durch Benutzername und Passwort (single signon). Die frei gegebenen Remote-Applikationen stehen über das G/On™ Menü direkt in der Taskleiste zur Verfügung (rotes [G] Symbol). Wird der Access-Key entfernt oder der Desktop Client beendet, dann schließt G/On™ sowohl Remote Session als auch die Anwendungen sofort.

Schritt 3
Die Anwendungskonnektivität stellt Ihr G/On™ Server über eine Single-Port-Protokollverbindung her, inklusive Prozesskontrolle (lock to process), die „silent“ arbeitet und auf Port-Scanning nicht reagiert. Volle Integration in Active-Directory- Strukturen, Lastverteilung und Fehlertoleranz sowie zentrales Management komplettieren die „all-in-one” Remote Access Lösung.

Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech’s core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.

G/On 2 Faktor-Authentifizierung



Schematischer Ablauf

G/On Nodeless Client
USB Access Key
oder **Desktop Client**

G/On™ eClient ist unveränderbar auf der CD-Partition des USB-Access-Keys (unique EDC) oder bildet als Software-Client einen maschinenspezifischen EDC (EDC = EMCADS™ Data Carrier - eindeutige, sichere Hardwareidentifikation).

Der Software-Client ist monolithisch aufgebaut (single EXE), portabel und erfordert weder Installation noch Registryeinträge. Er nutzt nicht den Microsoft Memory Manager.

Verbindungsaufbau zum G/On Server

Der Schlüsselaustausch erfolgt über das EMCADS™ Protokoll mit 163 Bit starken ECC Schlüsseln.

G/On Server
Authentifizierung HARDWARE

1. Faktor: Hardware-Authentifizierung (Token)
"was Sie physikalisch besitzen müssen"

Ist Client EDC Nummer am Server freigegeben (adopt)?
NEIN: Zugriffsversuch protokollieren, Verbindung beenden
JA: weiter zur Authentifizierung des Users

G/On Server
Authentifizierung BENUTZER

2. Faktor: Authentifizierung des Users
"was Sie wissen müssen"

Anmeldung mit *Benutzername und Passwort*
- Remote-User gegen AD oder interne DB verifizieren
- Prüfen der Zugriffszone
- G/On™ Anwendungsmenü gemäss Richtlinie und Gruppenzugehörigkeit zur Verfügung stellen

Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.

Vorteile von G/On gegenüber VPNs

Komplexität versus “easy-of-use”

Traditionell setzen Unternehmen für den Transport sensibler Daten über das Internet oder öffentliche Netze auf VPN-Technologien, die sie entweder selbst aufbauen oder von externen Dienstleistern anmieten. Entgegen der landläufigen Meinung sind solche Umgebungen jedoch keineswegs „plug & play” einsetzbar sondern erfordern eine umfassende Planung unter Berücksichtigung aller Kommunikations- und Sicherheitsanforderungen.

Verschiedene Produkte unterschiedlicher Anbieter müssen kombiniert werden, um jeweils verschiedene Teilbereiche des Verbindungsproblems zu lösen. Neben den reinen Client- und Rolloutkosten fallen schnell weitere Investitionen für Token-Server, Zertifikatserver, DMZ, Intrusion Detection- und Identity Management Systeme usw. an. Dies wirkt sich nicht nur nachteilig auf die TCO aus, sondern führt aufgrund der komplexen Topologie zu einem erhöhten Administrationsaufwand.

Das VPN-Dilemma

Führende Experten und Sicherheitsanalysten publizieren immer wieder umfassende Checklisten für Administratoren, die VPN-Technologien einsetzen möchten. Solche Empfehlungen sollten sorgfältig befolgt werden, um potenzielle Angriffsmöglichkeiten auf die Infrastruktur zu minimieren.

Leider sieht die Realität so aus, dass die angesprochenen Themen (und folglich auch VPNs ganz allgemein) das genaue Gegenteil von „einfach“ sind: Kompliziert, mit aufwändiger Wartung und massiven Einschränkungen für die Anwender verbunden. Administratoren stehen vor dem Dilemma, dass Unternehmen einerseits einen elementaren Bedarf an Remote Access Anbindungen haben, andererseits die publizierten “Tipps” in Wirklichkeit eine Aufzählung von Gründen sind, weshalb man VPNs besser nicht implementieren sollte.

Warum VPNs nicht wirklich “einfach” sind...

Exemplarisch möchten wir einige der publizierten Tipps und Tricks für den “sicheren Einsatz” von VPNs betrachten. Sie werden selbst feststellen: Einfach ist anders.

- **Verwenden Sie die stärkste verfügbare Verschlüsselung**

Die VPN-Verschlüsselungsverfahren sind vielfältig und derzeit gilt nur das L2TP (Layer 2 Tunneling Protocol) als sicher. Allerdings sorgt bei diesem Protokoll der Datenoverhead zur Absicherung für eine etwas langsamere Performance als beim unsicheren PPTP (Point-to-Point Tunneling Protocol).

✓ **G/On** verwendet keine Tunnelingprotokolle sondern hoch-performante Datenpakete mit 256 bit AES Verschlüsselung.

- **Limitieren Sie den VPN Zugang**

Eine oft ausgesprochene Empfehlung lautet: Geben Sie den VPN-Zugang nur dann frei, wenn er für Unternehmenszwecke unbedingt erforderlich ist. Anwender sollten darüber nicht mehrfach täglich Ihre Mails usw. abrufen.
Diese “Empfehlung” basiert auf der Tatsache dass VPN-Verbindungen immer eine Türe in das Netzwerk öffnen. Ist ein Anwender erst einmal Mitglied im LAN, müssen maximale Vorsichtsmassnahmen getroffen werden, damit eine Kompromittierung möglichst ausgeschlossen ist.

✓ **G/On** baut aus genau diesem Grund keine IP-Verbindung in das Netzwerk auf und kann deshalb jederzeit ohne Sicherheitsrisiko durch jeden Anwender genutzt werden - auch zum täglichen Mailabruf.

- **Implementieren Sie starke Passwort- und Authentifizierungsrichtlinien**

Wenn VPNs nicht durch zusätzliche Authentifizierungsmethoden, wie z. B. Smartcards oder biometrische Verfahren erweitert werden, dann ist die Sicherheit nur so gut, wie das “schwächste” Passwort. Experten empfehlen deshalb den Einsatz zusätzlicher, kostenintensiver Authentifizierungslösungen sowie den regelmässigen Austausch von Zugangspasswörten. Solche Verfahren reduzieren allerdings den Komfort für die Anwender erheblich.

✓ **G/On** beinhaltet bereits eine 2-Faktor-Authentifzierung im Basisprodukt und sichert den Remotezugang ohne 3rd-Party-Tools trotz einfachster Bedienbarkeit umfassend ab. Der Anwender benötigt lediglich seinen USB Access Key sowie Benutzername und Passwort.

Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech’s core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.

- **Stellen Sie den PC während der VPN-Nutzung unter "Quarantäne"**

Beim Herstellen der VPN-Verbindung und auch während der Sitzung sollten möglichst alle anderen Verbindungen auf dem Computer deaktiviert sein (kein Internetzugriff, keine voller Netzwerkzugriff). Ausserdem sollte der PC vor der VPN-Nutzung in folgenden Bereichen auf Einhaltung der Netzwerk-Policies überprüft werden: Ist eine aktuelle Antivirensoftware aktiv, sind Antispam-Signaturen aktuell, sind alle Patches/Hotfixes/Servicepacks eingespielt und ist sichergestellt, dass keine Fernwartung oder sonstige Remote Access Software aktiv ist?

Durch Einschränkung der Möglichkeiten sowie eine umfassende Prüfung wird Sicherheit für den User erreicht. Der Administrator ist gefordert, die für den VPN-Aufbau genutzten Computer regelmässig auf Aktualisierungen zu prüfen und Patches einzuspielen.

✓ Für **G/On** ist die Endpoint-Security nicht relevant, denn es wird keine IP-Verbindung in das LAN/WAN hergestellt. Auf dem Computer muss nichts deaktiviert werden - und da G/On keine Spuren hinterlässt entfällt das Löschen temporärer Dateien bzw. des Caches nach der Sitzung.

- **Sorgen Sie für maximale Sicherheit privater WLANs**

Mitarbeiter, die von zu Hause aus arbeiten, nutzen dort oft eigene Laptops und private WLANs. Da diese Zugangspunkte oft nicht ausreichend gesichert sind sondern einfach aus der Box in Betrieb genommen werden, muss der Administrator vor Ort für ausreichende Sicherheit sorgen, das private WLAN absichern und dafür sorgen, dass die Settings möglichst nicht verändert werden.

Soll vielen Mitarbeitern ein Homeoffice-Zugang eingerichtet werden, dann sind Einweisung und Vor-Ort-Konfiguration aufwändig und kostenintensiv.

✓ **G/On** nutzt ein WLAN lediglich als Zugangspunkt in das Internet. Da der Heim-Computer nie Mitglied im Firmennetzwerk wird sondern nur eine Applikationsverbindung über den G/On Server aufbaut und sämtliche Informationen durch EMCADS™ geschützt übertragen werden, kann auch eine unsichere Verbindung oder ein "untrusted" PC ohne jedes Sicherheitsrisiko für den Remote Access genutzt werden.

- **Mitarbeiter müssen firmeneigene Notebooks nutzen**

Für maximale Sicherheit sollten VPN-User mit firmeneigenen Laptops ausgestattet werden, die vorkonfiguriert und durch entsprechende Mechanismen unveränderbar geschützt sind.

Ungeachtet der hohen Anschaffungskosten wird auf diesem Weg nicht nur die Nutzbarkeit eingeschränkt, oft müssen Mitarbeiter dadurch mit mehreren Geräte arbeiten.

✓ **G/On** ist mit jedem beliebigen Computer nutzbar, der über einen USB-Port und eine Internetverbindung verfügt, ohne dass die Sicherheit kompromittiert wird. Da der Client auf dem USB Access Key ausgerollt wird, können Mitarbeiter, die bereits über einen Notebook oder PC verfügen, in wenigen Minuten mit einem vollwertigen Remote Access ausgestattet werden.

- **Setzen Sie wo immer möglich Intranets oder Extranets anstelle von VPNs ein**

Wenn Mitarbeiter nur auf bestimmte Dateien zugreifen sollen, dann ist eine mit sicherer Passwortauthentifizierung versehene Website sinnvoll, denn sie skaliert besser als VPNs und legt das gesamte Netzwerk nicht nach außen offen.

✓ **G/On** eröffnet vielfältige Möglichkeiten des Datei-zugriffs, ohne dass eine IP-Verbindung in das Netzwerk hergestellt werden muss. Es ist nicht einmal notwendig zu wissen, von welchem Server einzelne Dateien stammen, denn die Verwaltung übernimmt der G/On Server.

G/On ist die Alternative

Unsere oben dargestellten Praxisempfehlungen stehen stellvertretend für eine Vielzahl an Aufgaben, die Administratoren beim Einrichten einer VPN berücksichtigen müssen. Dies bedeutet in der Praxis, dass Einsatz und Nutzung einer solchen Technologie oft mit höheren Kosten, größerem administrativen Aufwand und gleichzeitig vielen Einschränkungen für die User verbunden sind.

Im Vergleich mit traditionellen VPNs ist G/On eine bemerkenswert einfach zu nutzende und gleichzeitig leistungsstarke Plattform, die das Arbeiten via Remote Access positiv verändert. G/On eliminiert bereits im Vorfeld viele Probleme, die in Zusammenhang mit der Absicherung von Endpunkten und der Netzwerkinfrastruktur gelöst werden müssen. Anwender verbinden direkt, absolut sicher auf ihre Applikationen, während Administratoren vom komfortablen Deployment und einem deutlich reduzierten Verwaltungsaufwand profitieren.

Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.

	IPSec VPN	SSL VPN	G/On
Erforderliche User-Rechte			
zur Installation	Admin	User + Rechte für Plugins	Gast
zur Ausführung	User	User	Gast
Authentifizierung			
Hardware Authentifizierung	Drittanbieter	Drittanbieter	integriert
Benutzer Authentifizierung	Ja	Ja	ja
"Trusted" PC erforderlich	Ja	Nein, aber empfehlenswert	Nein
Schutz vor Phising	Ja, (pre-shared secrect)	Ja, über Zertifikate	Ja, echte gegenseitige C/S Authentifizierung
Zugriffssicherheit			
Autorisierung	Drittanbieter	Drittanbieter	integriert
Sicherheitszonen	Nein	Nein	Ja
Active Directory Anbindung	herstellerspezifisch	herstellerspezifisch	integriert, optional
Lokales User-Management	herstellerspezifisch	herstellerspezifisch	integriert, optional
verwertbare Endpunkt-Daten (z.B. Passworte im Cache)	Ja	Ja	Nein
Daten-Verschlüsselung	max. 256 bit AES mit statischen Keys	SSL (typisch 128- max. 256-bit AES mit statischen Keys)	256 bit AES mit wechselnden Keys während der Session, 163 bit ECC während Aufbau
Schutz gegen "man-in-the-middle" Angriffe	Ja wenn das "pre-shared secret" gut geschützt ist	Ja, wenn Zertifikat gut geschützt ist	Ja Prüfsummen und angehängte Zeitstempel für jedes Paket
verwendete Tunneling-Protokolle	L2TP, P2PP und andere je nach Hersteller	L2TP, P2PP und andere je nach Hersteller	keines
Absicherung der Endpunkte			
Antivirus	erforderlich	erforderlich	empfohlen
Firewall	erforderlich	erforderlich	empfohlen
Client-Filterung	MAC/IP-Adresse	MAC/IP-Adresse	Hardware EDC und mehr
unerwünschte Prozesse, Malware-Prozesskontrolle	Drittanbieter	Drittanbieter	integriert, lock to process
Verteidigung gegen Angriffe	DMZ oder Applikationsserver	DMZ oder Applikationsserver	direkt auf der Client-Seite ausserhalb des Unternehmens
Access Layer			
Art des Zugriffs	Netzwerkebene	Netzwerkebene	Applikationsebene
Mitglied im Netzwerk	Ja	abhängig vom Produkt und Setup	Nodeless-Client, keine IP-Verbindung ins Netzwerk
Offene Ports	mehrere	mehrere	einer
Sonstiges			
Administration und Verwaltung	dezentrale Verwaltung über Tools und Browser, sowie Programme von Drittanbietern	dezentrale Verwaltung über Tools und Browser, sowie Programme von Drittanbietern	zentrale Verwaltung nur über den G/On Server
Infrastruktur	typischerweise 2 bis 4 Hersteller	typischerweise 2 bis 4 Hersteller	1 Produkt (all-in-one)

Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.

Der G/On USB Access Key

Ihr hochsicherer Schlüssel zum Remote Access

Der hochwertige G/On USB Access Key bietet mobilen Anwendern maximale Flexibilität, da nur ein Computer mit Internetverbindung und USB- Steckplatz erforderlich ist, um eine Remote Session aufzubauen.

Der Client ist auf der Read-Only Partition des USB Access Keys eingebrannt und so konfiguriert, dass er nach dem Einstecken automatisch startet (auto launch). Sobald die Login-Dialogbox erscheint, kann die Verbindung durch Eingabe von Benutzername und Passworts aufgebaut werden. Die freigegebenen Applikationen stehen Ihnen dann über das G/On Menü in der Taskleiste sofort zur Verfügung. Für jeden Access Key ist eine G/On Client-Access Lizenz (CAL) erforderlich.

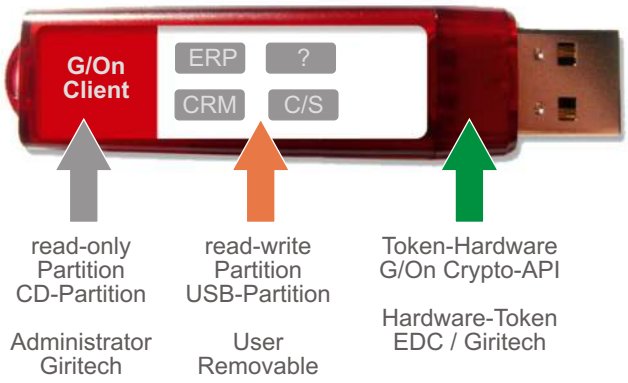
Vorteile des USB Access Keys

Vertrauenswürdige Anwendungen können in die sichere G/On-Verbindung eingebunden und auf dem USB Access Key abgelegt werden (wahlweise auf der unveränderbarer CD- oder veränderbarer Read/Write-Partition). Die Session wird mit Abziehen des G/On USB Access Keys automatisch beendet, ohne dass Spuren auf dem PC zurückbleiben - weder Informationen im Cache noch temporären Dateien (Zero Installation + Zero Bootprint).

Herausragende Sicherheit

Da der G/On USB Access Key eine Token-Funktion erfüllt, ist er in Verbindung mit Password und Benutzername Ihr Schlüssel für den Applikationszugriff. Geht der Key verloren, dann kann er durch den Administrator sofort deaktiviert werden - und ohne Zugangsdaten kann ein potenzieller Dieb nichts damit anfangen.

Damit Anwender in Hochsicherheitsumgebungen den USB Access Key nicht als Speichermedium "missbrauchen" können, lässt sich die beschreibbare Partition auf ein nicht mehr nutzbares Minimum verkleinern und auf Wunsch so absichern, dass der Zugriff auf diesen Bereich explizit über den G/On Server autorisiert werden muss. Das Kopieren von Dateien über den Access Key wird dadurch ebenso wirksam unterbunden wie das Aufspielen von unerwünschter Software.



Übrigens kann nur der G/On Server, an dem der Access Key aktiviert worden ist, diesen verwalten oder dessen CD-Partition beschreiben.

Warum wird für G/On kein "normaler" USB Stick verwendet?

Grundsätzlich ist der G/On Access Key Ihr “Schüssel” zum Remote Access und damit ein entscheidender Sicherheitsfaktor - ähnlich wie ein Firmenschlüssel.

Der Key enthält einen fest eingebrannte Hardware-Token (EDC), der von G/On zur eindeutigen Identifizierung der Hardware verwendet wird. Dies ist ein wichtiges Element der integrierten 2-Faktor Authentifizierung und besonders in Umgebungen wichtig, in denen kein vertrauenswürdiger Computer verfügbar ist: Hier dient der USB Access Key zum gesicherten Transport des Clients auf der (nur durch den G/On Server veränderbaren) CD-Partition. Zusätzlich benötigte Anwendungen oder mobile Clients lassen sich bequem auf der RW-Partition ablegen und sogar vom G/On Server aus auf den Key übertragen.

Außerdem schützt die CD-Partition vor Fehlbedienungen, wie versehentlichem Formatieren, denn der Access-Client bleibt immer unveränderbar auf dem Key vorhanden. Dadurch kann der Key jederzeit aus der Ferne über den G/On Server wieder hergestellt, gelöscht und/oder neu bespielt werden.

Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.

Verwaltung der G/On USB Access Keys

Alle ausgegebenen Access Keys werden zentral über den oder die G/On Server verwaltet. Im Administrationsmodul hat der IT-Verantwortliche jederzeit Zugriff auf eine Übersicht aller aktivierten (”adopted”) Access Key, kann den aktuellen Status abfragen, die Anzahl fehlgeschlagener Verbindungsversuche einsehen und vieles mehr.

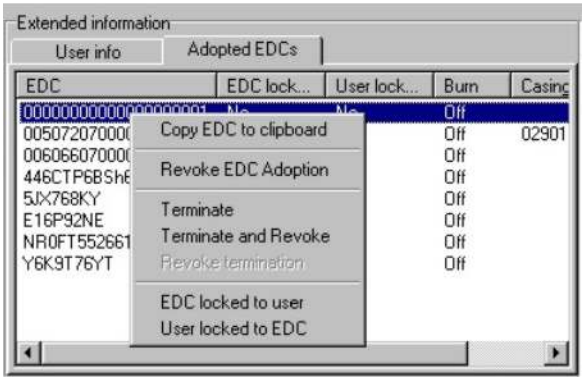
Falls ein USB Access Key verloren geht oder aus anderen Gründen deaktiviert werden muß, dann stehen dem Admin folgende Optionen zur Verfügung:

Revoke entfernt die Hardware-ID vom Server die Authentifizierung schlägt somit fehl und der User kann mit dem Gerät nicht mehr verbinden

Terminate löst einen logischen Kurzschluss auf dem Chip des USB Access Keys aus, d. h. der Key wird vollständig zerstört und kann weder weiterhin genutzt noch reaktiviert oder repariert werden

Die Kombination “**Terminate and Revoke**” führt zuerst den Terminate-Befehl aus (Key wird unbrauchbar) und entfernt danach die EDC Nummer vom G/On Server.

Einzelinformation pro G/On Access Key ink. Login-Informationen und Status.



Die verfügbaren Aktionen pro EDC Device erlauben die Zuordnung eines Gerätes zum User und umgekehrt. Ausserdem kann ein EDC Device gesperrt und bei USB Access Keys sogar terminiert werden.

Giritech GmbH · Mariabrunnstr. 123 · 88097 Eriskirch · Tel. +49 (0) 7541 971099-0 · Fax 971099-99 · info@giritech.de · www.giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech’s core intellectual property includes the patent-pending systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. All rights reserved. Copyright © Giritech GmbH November 2008.