Talk2M and eWON

Architecture for Industrial Remote Access

A general description v3.0

Providing Remote Access
in the world of automation

The provision of industrial remote access systems for Machine builders and OEMs is becoming a standard way of connecting remotely to an automated system or a machine. In less than eight years, Internet Remote Access has entered the world of Automation engineers to replace telephone connections as the means of access to a system, and words such as "Industrial Router" and "VPN" are now in common usage in service organizations.

There are already several Internet Remote Access offers on the market. In the For Dummies eBook 'Secure Remote Access for Industrial Machines', we underline all the benefits of a web-based remote access architecture. Indeed, a cloud architecture is the perfect place to connect VPN-based communication generated by users on one side to VPN-based communication generated by machines on the other side. VPN communication is a part of everyone's life today, when we use the Internet to gain access to private resources, such as in a business environment to link our PC to an Office central server.

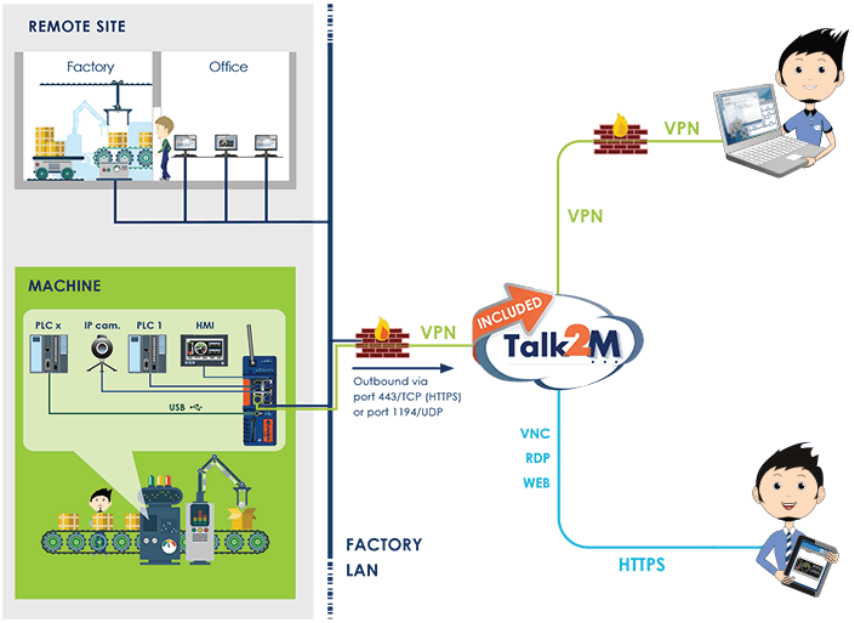
In this paper, we aim to describe in greater detail our paradigm of a Cloud Platform that we have created at eWON: Talk2M. This document is not intended as a User guide or manual. If you need a manual for Talk2M, we suggest you visit the following link:
http://ewon.biz/support/product/talk2m/talk2m

What are
VPNs and tunneling?

VPN (virtual private network) and tunneling are techniques that allow, among other benefits, to encrypt data links between yourself and another computer. This computer might belong to your organization, a trusted person or organization, or a commercial VPN service. Tunneling encapsulates a specific stream of data within an encrypted protocol, making everything that travels through the tunnel unreadable to anyone along the transmission path. Using a VPN or other form of tunneling to encrypt data is one of the best way to ensure that it will not be seen by anyone other than you and people you trust. Another major benefit of this technique is the authentication of remote parties.

What is Talk2M?

Talk2M proposes internet-based connectivity services to connect users to their machines via the Internet. These users are typically Service or Automation engineers who need access to their machines installed on several customer premises, usually spread all over the world.
On the user side, we need to install a software application that runs on a PC with the Windows operating system. This client application, named eCatcher, establishes, a seamless communication link between the PC and Talk2M, through the Internet. We will also see that a simple web browser can be used to connect to the machine, thereby avoiding the need to use the client application, but this is limited to certain applications.
On the machine side, we install an eWON industrial gateway (Cosy, Flexy, CD) connected to the heart of the machine, a PLC (Programmable Logic Controller), an industrial PC or any automated device – inside a factory plant.
The eWON is connected to the machine either through an Ethernet four-port switch, a USB link or a serial link (RS485/232 or Siemens MPI type).



Picture 1: Talk2M communication overview

Between the eWON router and the user we provide TalK2M, a cloud-based communication structure made of several servers which relay the communications originated by the users to their machines. The entire system operates with the prerequisite that both sides of the communication can access the Internet and reach the Talk2M servers.
We begin by describing the possibilities from the machine side of reaching the Internet, and how this is done.

How do you connect
the machine to the Internet?

As already mentioned, the machine side needs to be connected to the Internet in order to reach the Talk2M server. They are many ways to reach the Internet:

- The most used and cost-free way is to pass through a LAN network connected to the Internet. If the LAN is not connected to the Internet (e.g. closed LAN) or no LAN connection is available, we can usually use the second or third way.
- A second way that we see developing in factory plants is with WiFi connectivity. Some factories provide WiFi hotspot networks intentionally for machines builders to get access to Internet without passing though their corporate LAN for remote connectivity.
- The third way is usually the contingency way when NO LAN or NO WiFi are available.
- Cellular technologies (3G, 4G) are available worldwide and provide a very practical way to connect to the Internet. In this case, we would need a SIM card from a mobile phone provider to allow our cellular router to connect to the Internet.

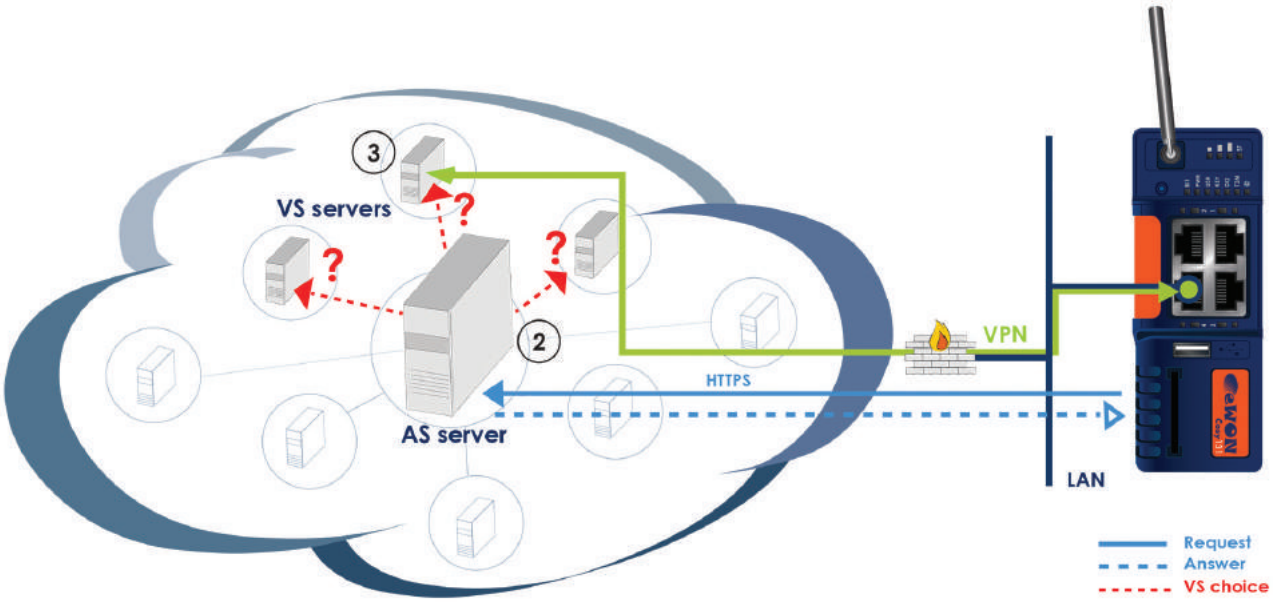
According to the eWON model, the Internet connection is established through a WAN connection, provided either by an Ethernet Interface or a built-in modem (cellular, WiFi, ADSL or PSTN). Some eWON models can also provide both an Ethernet interface and a built-in modem. Of course, you can also use an external modem such as CDMA, satellite or radio technologies.

Choice	Connection type	Advantages	Drawbacks
1st	LAN	Found on almost every site Cost of usage is free High bandwidth	LAN can sometimes be closed because of security policy
2nd	WiFi	Cost of usage is free High bandwidth	Growing technology, however expect limited availability
3rd	Cellular	Worldwide availability Cost is data dependent	High speed is not available everywhere. Technology may vary around the world, requiring specific devices. Cost is not free

Connecting the machine
to Talk2M

Once connected to the Internet, the first thing that the eWON will do is to connect to the Talk2M servers. The connection of a machine to Talk2M is performed in three phases:

1. A first and initial commissioning process where the eWON will connect to a central Access Server (AS) and authenticate through an HTTPS connection. It will then fetch its certificates. This operation is executed once, then the eWON will save its key and certificates internally. This point will be explained later in this document.
2. Then, every time the eWON needs to connect to the VPN, it will first ask for the Hostname of the VPN server (VS) it needs to use (this VPN server address may change at any time from connection to connection). This request is also sent via an HTTPS connection.
3. Finally, the eWON will set up a VPN tunnel with the VS assigned in the previous step.



Picture 1: Talk2M communication overview

Connecting the user
to Talk2M

As already mentioned, the first step is to start eCatcher software on the user's PC. When started, eCatcher will require the user to authenticate himself with three important pieces of information:

- **An Account name:** a Talk2M account can be created with eCatcher. Anyone can create an unlimited number of Accounts. Each account contains all Users who can connect in the same context to all eWON devices registered in that Account. User A from Account X will never be able to connect to a device from Account Y. But User B of Account Y will be able to connect to this device.
- **A Username:** it is recommended to not share accounts and instead to create individual usernames for each person accessing the account. With both Talk2M Free+ and Talk2M Pro you can create as many users as needed, at no additional cost.
- **A password:** each user has his own password, which can be changed by the administrator or any user who has the right to change the User's password.

Once authenticated, the user obtains access to the list of all eWONs registered in that account.

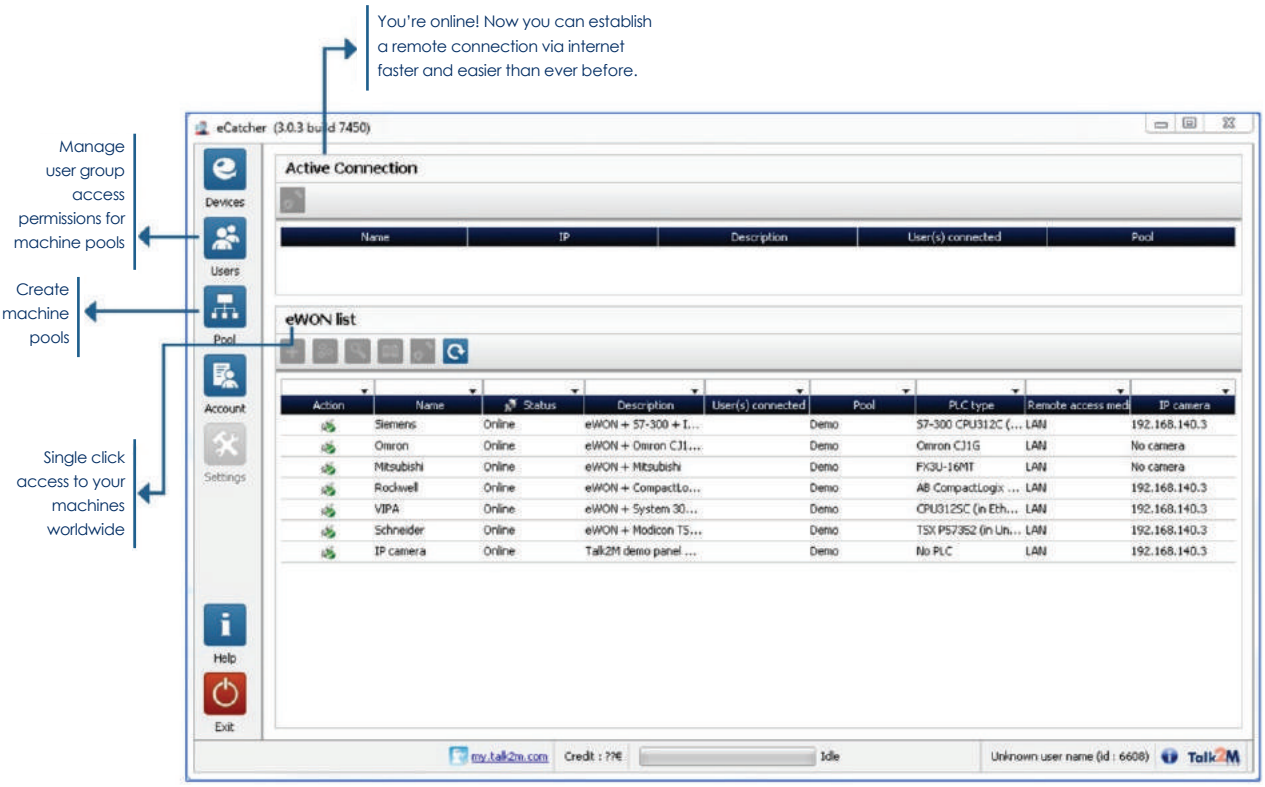
This stage is equivalent to phases 1 and 2 described in the previous section. This means that eCatcher will not save its key and certificate locally, but will fetch them after each authentication. In fact, eCatcher opens an HTTPS session on the AS. The user can perform several actions, such as (from the button displayed on the left-hand side):

1. Registering a new eWON in the current account. We will describe this operation in the following paragraphs.
2. Modifying and deleting eWON information
3. Adding, modifying, or deleting User information or groups in the current account. A group is a collection of users.
4. Adding, modifying or deleting Pools in the current account. A pool is a collection of eWONs.
5. Modifying the account information.

Note: Point 1 will be explained later in this document. Points 2 to 5 can be easily found in the Talk2M User's guide (see **https://ewon.biz/support/docs/talk2m** , our support page regarding all Talk2M features).

When clicking on any eWON listed (see picture 3) and if the eWON Connection status is set to Online (meaning a VPN with the eWON is possible), eCatcher asks the AS to open a VPN tunnel. As in the previous paragraph in phase 3, the AS indicates to eCatcher which VS will be used to establish a VPN connection.

But in that case, it is the VPN Server already used by eWON with its VPN tunnel connected. So eCatcher starts its VPN tunnel to the VS that has been assigned by the AS. Both VPN end terminations are therefore automatically linked together on the same VS.



Picture 3: eCatcher with its list of connected devices

We will discuss eWON Off-line status, meaning non-permanently connected, later in this document.

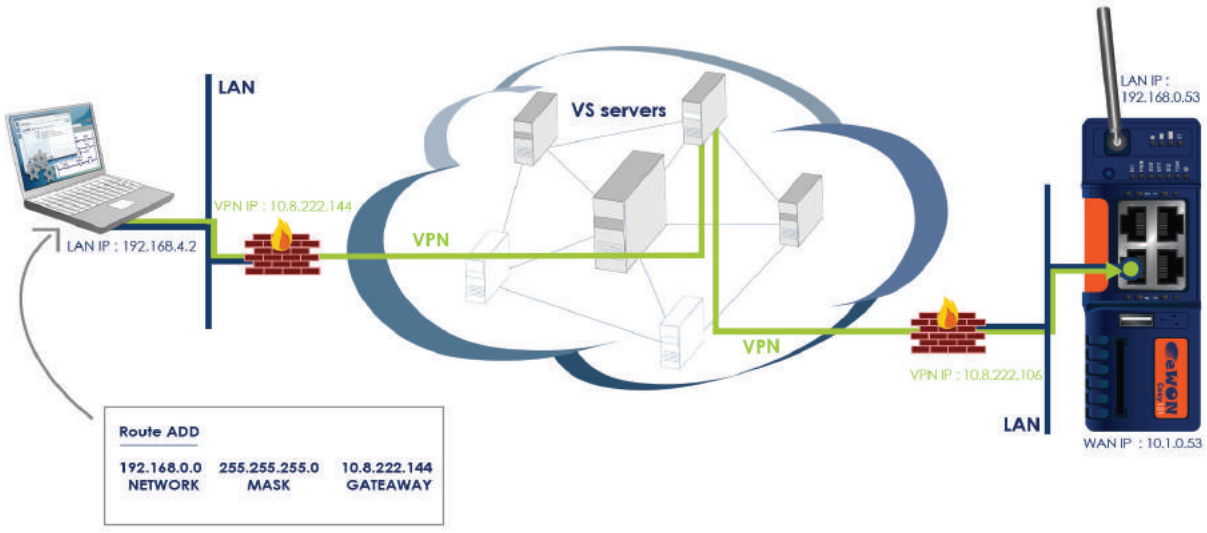
Using the VPN connection

In the two previous paragraphs, we described how connections from one end – the user – to the other end – the machine – are possible.

Both VPN connections, when created, are assigned with a unique VPN IP address provided by the AS via the VS among the server farm. While the VPN addresses are visible from the eCatcher side and on the eWON side, the VPN addresses of both tunnels on the VS side are not visible.

On the eCatcher side, the VPN address provided is assigned to a TAP Win32 adapter. This adapter provides a virtual interface that connects the PC directly to the VS. The TAP interface is installed automatically by the eCatcher installation program.

Having access to the VS (through the TAP interface) is not the final goal; in fact, we need to reach the machine side of the eWON (in other words), the LAN. We must therefore indicate to the PC that all IP messages containing a destination address belonging to the eWON LAN IP address range should be forwarded through the TAP interface. To allow this, a route is automatically added by eCatcher when a VPN connection is opened. This route is deleted when the VPN connection is closed or destroyed. The Network destination address is known thanks to the configuration information contained in each eWON Talk2M entry. The LAN address is mentioned when an eWON registers itself into a Talk2M account. If the user wants to connect to another eWON, the previous route will be destroyed, and a new route will be added with the appropriate destination address range.



Picture 4: VPN Connection from one end to the other end, with all IP addresses involved

On the machine side, the IP traffic coming through the VPN tunnel is forwarded to the LAN side of eWON automatically. If a device on the LAN wants to reply to the PC, there are two possible strategies:

- a NAT (Network address translation) on LAN feature, also called Plug'n Route, substitutes the eWON IP LAN address for the PC IP address. This is the default configuration in the eWON. See picture 5 for a brief explanation.
- Every device on the LAN side should have the eWON configured as its gateway, which requires reconfiguring the IP address setting of each LAN device. While this is the least preferred strategy, it might be required in some advanced configurations regarding Internet routing.

VPN technology used

Talk2M VPN protocols are based on Open SSL and Open VPN. OpenVPN is intended to use UDP on port 1194 by default, however we also use TCP 443 (HTTPS). For the VPN, eCatcher and eWON use both ports for tunneling.
One effect of using TCP 443 inside LAN will be the possibility of having to pass through HTTP proxies. This will require proxy authentication settings to be provided on both the user and the eWON side.
Proxies that are supported both by eCatcher and eWON routers are:

- Proxy without authentication
- Proxy with user and password authentication
- NTLM Authorization proxy

Registering an eWON Router into a Talk2M Account

Registering an eWON inside TalK2M requires two steps:

1. The first step is to create an eWON entry in the context of an account, with three registration options.
2. The second step consists in running the Talk2M connection wizard inside an eWON, which will connect to Talk2M for the first time and complete the registration process. This step can also be done during the commissioning of the eWON on a customer site, completely or partially (if the eWON has been preregistered in the factory, we only need to check the internet connection).

The three registration options are:

- via activation key: Most common way of registering a new eWON entry in Talk2M. Talk2M generates a unique activation code which will be used by the eWON in its registration phase with Talk2M.
- via eWON Name: This is a contingency way of registering an eWON when an eWON is already on site and has not been yet registered.
- via an SMS: The SMS contains the activation key; this method is thus similar to the first method. This is the "last resort" way of registering an eWON in case of a critical problem such a loss of communication. When the eWON receives the SMS, it will then automatically trigger the Talk2M connection wizard and will reconfigure itself to connect to the Talk2M servers.

During the wizard process, the first step of registration is the request to the AS for a certificate. It contains the private key and certificates needed by the encryption algorithms

The eWON registration process also assigns the eWON serial number to each certificate. While you cannot register two eWONs with the same serial number (the new registration will replace the old one), the system allows the duplication of the eWON configuration to another device in case of eWON replacement. In that case, Talk2M will check for certificate use exclusively.

Customer or end-user
keeping control on the machine side

Using a LAN connection usually means that the eWON gateway is permanently connected to the Talk2M server. There are cases, however, where machine builders' customers might be reluctant to leave the eWON gateway permanently connected, especially if remote access is rarely needed, or the customer wants full control over the connection.

We therefore suggest using a panel mount key switch which can be installed, for instance, on the front door of the machine cabinet. The switch can be wired to the eWON router digital input. On eWON Cosy models, the digital input, when set to 0 volt, disables the VPN connection. On other eWON models (Flexy, CD), the same result can be achieved, but through configuration pages. A digital output is also available to control a relay that can be used to physically decouple the Ethernet connection from the corporate network. This is probably the ultimate method for the machine builders to feel that they are in total control of the connection by turning the switch on & off.

There are also connection types which require other artifacts to start up the connection. When using a cellular connection, it is unnecessary to keep the VPN connection permanently up and running. Keeping a tunnel open requires the regular sending of "keep alive" messages, which increase the volume count on communication bills (1 or 2 MB per day).

During the first phase of registration, a user can declare which connection type the eWON router will use. In case a cellular connection type is chosen, a phone number input field needs to be completed. This phone number can then be used to send an SMS message to an eWON. Upon reception of this SMS message, the eWON will connect to its cellular network provider and by extension will connect to the Talk2M connectivity services to start the VPN tunnel.

Phone connection type is by definition non-permanent, and you therefore need to dial the eWON router in order to connect to its Internet service provider (ISP) first, to then set up the tunnel.

Security of the Talk2M
System and Architecture

Security is probably the most important aspect of the Talk2M architecture. To achieve this, we have elaborated a security philosophy based on a "Defense in Depth Approach" (DPA - see picture 6). The DPA is a coordinated use of multiple security countermeasures spread on a multiple layers of security controls. The purpose is to ensure T2M platform security and so confidentiality, availability and integrity.

Picture 6. Defense-in-Depth Approach

It is based on guidelines set forth by leading security standards like ISO27001, IEC 62443-2-4 and NIST Cyber Security Framework 1.0 in addition to numerous other publications, guidelines and industry best practices.

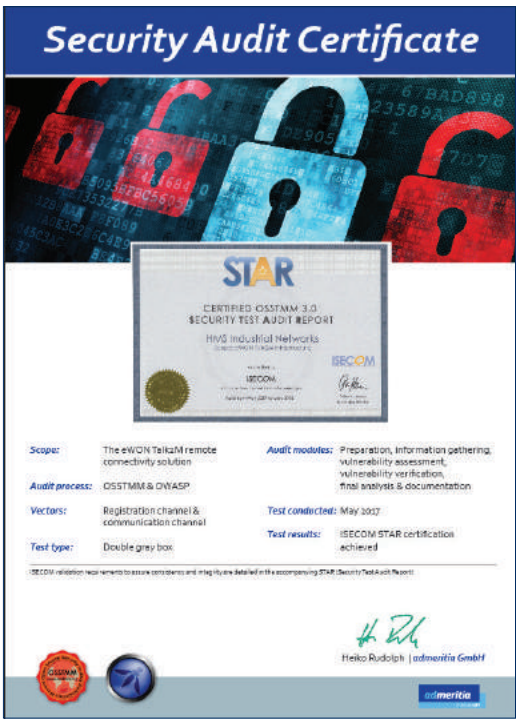
Here is a description of the different layers starting from the inner layer to the outer layer and the security aspects implemented on each of these layers.

Layer	Layer Name	Security aspect implemented
1	eWON Device	1. eWON configuration: users should pass through the eWON authentication security, requiring at least eWON administration rights. 2. Network segregation: traffic on the machine/LAN side is segregated from the WAN/customer side (NAT 1:1). Users can only access authorized devices on LAN. 3. The device authenticates itself to the Talk2M platform 4. Physical Switch to control Internet connectivity.
2	Firewall	Filtering/Firewalling: up to 4 filtering levels are possible, allowing the filtering of a user's traffic to any Ethernet devices, any USB/serial devices or even any internal eWON services. The filtering is managed and applied on the TalK2M connectivity platform itself and not in the eWON router.
3	Traffic Encryption	Users and eWON routers are authenticated by the AS using TLS for HTTPS session authentication & data encryption. While connecting in VPN to the VS, the eWON uses the same TLS protocols & mechanisms for secure tunnel transport. Only secure ciphers are used.

Layer	Layer Name	Security aspect implemented
4	User & access management	1. Users & eWON Access controls: the purpose is to define which users can have access to which machines. This works through roles that you can grant to Groups and Pools to allow different access levels. 2. Unique User login with (optional): a. Password reinforcement policies, minimum length, requiring letter, digit and special char, expiration period, old password list b. Double factor authentication: after regular of login/password inside any account then a second window pops up, requiring SMS key 3. Connection Audit trail (who, when and how long) 4. User lockout implementation to prevent too many connection attempts from an unauthorized user trying to guess a password. 5. Digital key switch to keep local control
5	Talk2M Network infrastructure	eWON regularly assesses the Talk2M architecture as part of a Risk Management requirement. Appropriate controls are then put in place for compliance and effectiveness. We list below the different sections and control objectives of this assessment. a. Security policy: to provide Talk2M team with support for data security in accordance with business practice and relevant laws. b. Organization of data security: to provide a management framework for the implementation, monitoring, and control of the Talk2M security management system. c. Human Resources Security: To ensure that all employees understand their responsibilities and are suitable for the roles they are considered for, and to reduce the risk of misuse of the Talk2M system. d. Asset management (servers and internet infrastructure), Physical and Environmental Security: for this part, eWON is signing contracts with several hosting companies. For critical hosting part, eWON relies on Rackspace, due to ISO27001, SSAE16 type II SOC1, SOC2 (Security and Availability Only), and SOC3, which is the ultimate in hosting certification. The SSAE16 is an enhancement of SAS 70. It is an auditing standard designed to enable an independent auditor to issue an opinion on a service organization's controls. The SSAE16 audit report contains the auditor's opinion, a description of the controls in place, and in the case of a Type II audit, a description of the auditor's test of the effectiveness of the controls. e. Permanent Audit trail: All servers are audited by logging all operating information. eWON also implements continuous logging.
6	Policy compliance	The Talk2M remote access solution is designed to be compatible with customers' existing security policies. By using outbound connections over commonly open ports (443 and 1194) and by being compatible with most proxy servers, the eWON is designed to be minimally intrusive on the network and work within the existing firewall rules. So, no need to adapt your security equipment's configuration. Within eCatcher, Talk2M account administrators can customize the password policies to force compliance to corporate password policies and can restrict which users can access which devices remotely. Talk2M account administrators can also view the Talk2M Connection report to see which users are connecting to which devices and when. This report can be a valuable tool to ensure that that customer's corporate remote access policies are being followed.

Our Talk2M systems are regularly assessed by independent security testers in order to ensure that we keep a good security posture, and so we provide the highest security level to our customers. That's why in May 2017 we received our first security certificate, the STAR (Security Test Audit Report) certificate that is the result of a security assessment of the T2M environment by admeritia GmbH.

Having a good security posture is of course very important, but to maintain it, you need a good information security management system, focusing on risks, continual improvement and processes aspects! That's the responsibility of our security manager, who manages our security program from A to Z following the ISO27001 standard. HMS is ISO27001 certified for Talk2M since September 2017.



Availability of Talk2M servers

After security aspects, the second-highest priority of Talk2M architecture is to provide the best possible business continuity of its web connectivity services. Two kinds of service are proposed to customers:

- The Talk2M Pro offering, with a payable "mission-critical" service level agreement (SLA), or
- The Talk2M Free+ offering, provided for free connection services, as its name suggests.

The "mission-critical" service has been designed to provide Talk2M service business continuity of more than 99.6% over a one-year period, with a maximum breakdown of 4 consecutive hours on the AS for all Talk2M customers and on VS for Talk2M Pro customers only. To provide these two levels of service, Talk2M architecture is reinforced by several sections and control objectives such as:

1. Hosting provider SLAs: eWON has contracts with several providers. However, depending on the TalK2M services provided, eWON may deal with different providers.
    a. The Tak2M Pro "mission critical" services are hosted through our partner Rackspace, which can provide us with a 99.99% 24/7/365 guaranteed Internet Access and 1 hour maximum server breakdown time SLA.

    b. For the Talk2M Free services, we rely on several hosting partners which propose 99% or more SLA business availability, with longer potential breakdown time.

2. System Monitoring: we monitor the key performance indicators of all servers. All data acquired are displayed on a monitoring dashboard and are also logged on an alarm server that will send email and SMS notification messages to our 24/7/365 duty service personnel.
3. Server roll-out: with three different providers, and in case of major server breakdown, we can quickly roll out VPN connections from one VS to another VS in case of problems.
4. Continuous monitoring services: TalK2M Services are monitored by on-duty engineers according to a scheduled calendar.

Talk2M servers distributed globally

Another benefit is the distribution of our hosting sites. To reduce latency between IP packets, we have spread our sites in different regions of the world, such as Europe, the US and many other countries/regions (see picture 8 – VS deployed dated July 1st, 2015). We will gradually expand to other regions. This is required by some industrial PLC protocols which were designed with small-sized TCP/IP packets: In the case of slow internet connections and long internet distance between the user and his machine, these protocols are much more sensitive to the occurrence of timeouts.

Figure 8: VS available on the Talk2M network

We are therefore able to move at any time the VPN connectivity of an eWON router on is geographically closest VS. The eWON will then automatically reconnect to its new VS immediately.

Warning: Talk2M Server name must be opened explicitly in the End-User Proxy/FW:
Always open *.talk2m.com. Individual hostnames or IP addresses can't be used since those failover scenarios would not be supported.

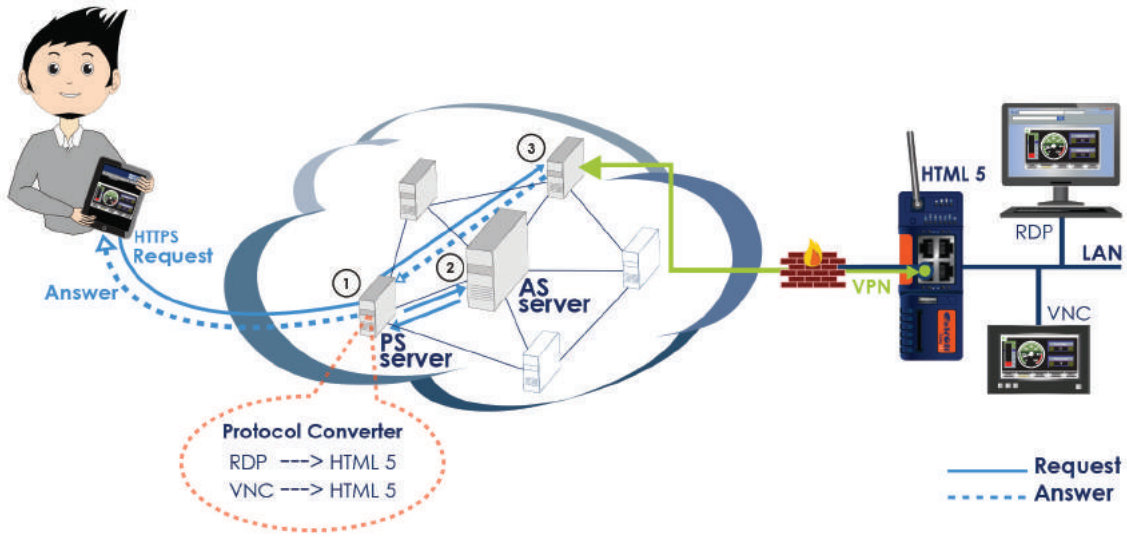
To allow quick connection between the various servers, all VS servers are connected to the AS through IPSec VPN tunnels.

M2Web, the Talk2M client
for HMI remote monitoring

Instead of using eCatcher, users can also connect through our M2Web portal, using a simple browser. This allows users to connect to the Talk2M server using HTTPS connections, without the need to install a specific application or software. With this service, anyone can connect to a machine with their web browser as a client though the portal https://m2web.talk2m.com. On the M2Web portal, the HTTPS traffic is redirected to the appropriate machine through its machine VPN, to finally reach the eWON router.
Because eWON routers have been designed to connect remotely to PLCs and automation devices, M2Web proposes to connect to HMI (Human Machine Interface) devices inside the machines, such as panels, PCs, or any device supporting HTML5.0 server page.
M2Web also contains a VNC (Virtual Network Computing) protocol and RDP (Remote Desktop Protocol) to HTML5.0 converters. VNC protocol is widely used in automation panels and RDP is provided inside Microsoft Windows Operating System platforms.

The connection to a machine from a browser in HTTPS is performed in 3 steps (see picture 9):

1. In the first step, the user triggers a hyperlink pointing to a page of the Web Proxy containing the account name, and an eWON name belonging to this account. Once the page is activated, the Web Proxy answers with an authentication window.
2. After being authenticated, the AS points out to the Web Proxy which VS server is used by the machine VPN tunnel.
3. All HTTP requests initiated on the client web browser and passing through the Web Proxy are redirected through the tunnel of the machine VPN and finally reach the eWON or any devices located on the LAN side and which support either HTML5.0, VNC or RDP protocols. This is made possible inside the eWON by enabling a port forwarding function (called 'Proxy').



Additional servers: SMTP relay, SMS gateway

TalK2M can also offer services other than remote access. SMTP relays and SMS gateway servers are also provided to our customers. Both are used to extend the notification mechanism provided inside the alarm system available in an eWON gateway. Every piece of data gathered into a PLC or industrial device connected to the eWON gateway can then be used to trigger alarm messages forwarded inside the VPN tunnel. At the output of the VPN tunnel, they can be relayed on the Internet as an email or a SMS.