M2U - Pushing data to customer server

Abstract:
M2U is a secure communication channel that allows to push data from eWON (or LAN device) to a customer server using HTTP

Project : M2U - Preliminary user documentation

Reference:

Revision: 01

Status: RELEASED

Last modification: 21/10/13

Author: Serge WAUTIER

eWON sa

Av. Robert Schuman 22 - BE-1400 Nivelles - BELGIUM
Tel +32 67 895 800 - Fax + 32 67 330 678

Table of content

1. Document information

File name : Build 24

Modifications History

Revision date	Modified Sections	Modification / Description	Author
26/03/2013 01	All	Document creation	Serge WAUTIER
12/04/2013 02	Many	Various clarifications and corrections	Serge WAUTIER
21/10/2013 03		Added a few clarifications	Serge WAUTIER

2. Introduction

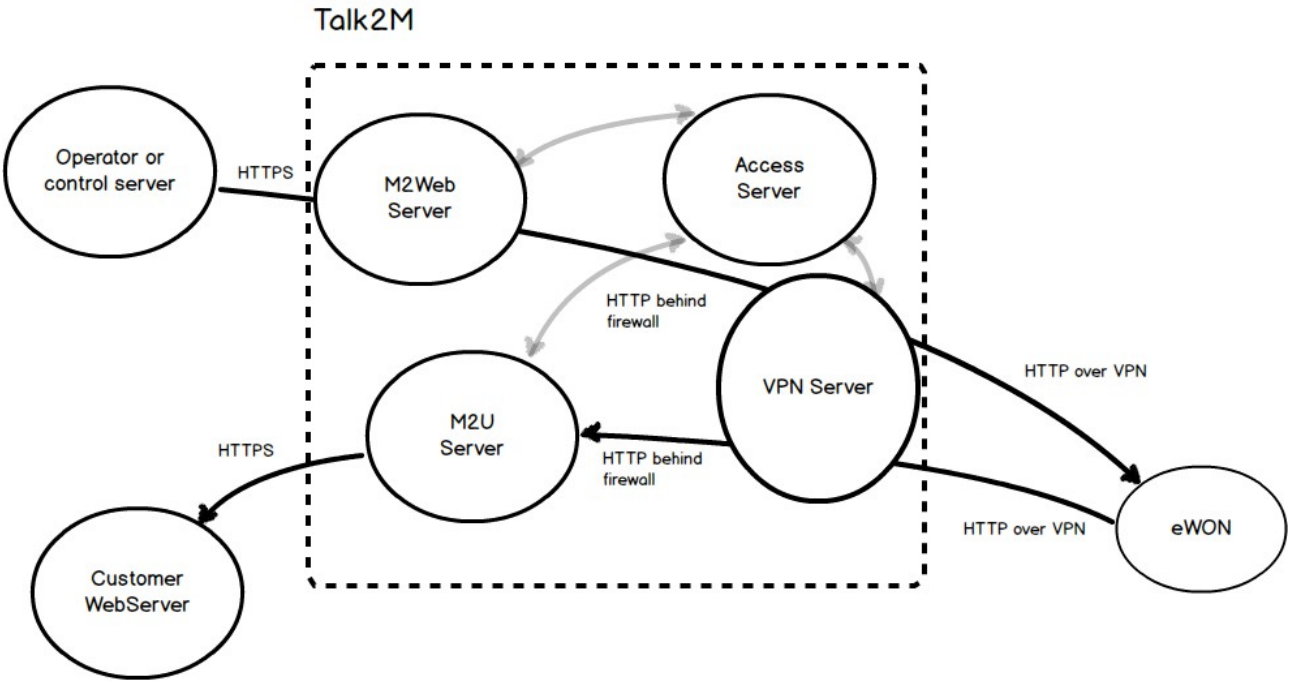
M2U stands for *Machine to You*.

It is a Talk2M service that lets eWON perform secure HTTP request to a customer's web server. Those requests typically push (POST) application data to the server but can also be used to retrieve information from the server (GET).

This can be seen as the opposite channel of M2Web: M2Web allows an external operator or process to initiate a (secure) HTTP connection to the eWON. M2U allows the eWON to initiate such a connection to the customer server.

The eWON actually connects the M2U server (a Talk2M server) which acts as a reverse proxy to the customer server.

3. Basic Architecture



eWONs send regular HTTP requests to the M2U server, which in turns forwards them to the customer server using HTTPS.

3.1 M2U Server

The M2U server stands as a man-in-the-middle aimed at hiding the customer server hostname from the eWON (centralized management) and securing the HTTP connection over to the customer server (out of Talk2M VPN).
eWONs send their HTTP request to m2u.talk2m.com.

4. Resolution of M2U hostnames

The eWON is able to resolve the M2U hostnames (e.g. m2u.talk2m.com) even without a DNS available.

IMPORTANT: Requires eWON firmware 7.0+ (6.4s6+ should do but no guarantee!).

5. Authentication of M2U Server

The M2U HTTPS client exposes a client certificate to the customer web server in order to allow authentication of the M2U HTTPS client by the customer server.

The certificate identifies the server as m2u.talk2m.com and is signed by a well-known authority, thereby allowing the web server to validate the certificate.

NOTE: This feature is not yet implemented. The M2U server does not expose any client certificate yet.

6. Control Usage of Customer Server

A Talk2M user is free to let its eWONs send data to any web server using M2U. There is therefore a possibility that a Talk2M user lets its eWON send data to the server of another customer and even forge the identity of an eWON to send fraudulous data.

This can of course be addressed by implementing authentication mechanisms in the HTTP request emitted by the eWON (either using standard HTTP authentication mecanisms such as Basic Authentication ot by simpler means such as a login specified in the POSTed data or through the request parameters (query string).

However, in order to simplify the eWON application, M2U implements the following features that help restrict the use of a customer web server by other Talk2M users:

- Talk2M eWON identification (account ref + eWON's name and S/N) are sent to the server using a custom HTTP header.

  X_Talk2M_Account
  X_Talk2M_Device
  X_Talk2M_SerialNumber

  This lets the customer server check that the request comes from an authorized account.
  Although these headers are filled in by default, the Talk2M account administrator may choose not to send this information to the remote web server (See *Expose eWON identity to 3rd party server* setting). If this option is unchecked, the headers are sent with an empty contents.
  Talk2M ensures that these headers are not forged by the eWON.
  It is not recommended to rely on the eWON serial number since it would change in case the eWON need to be replaced.

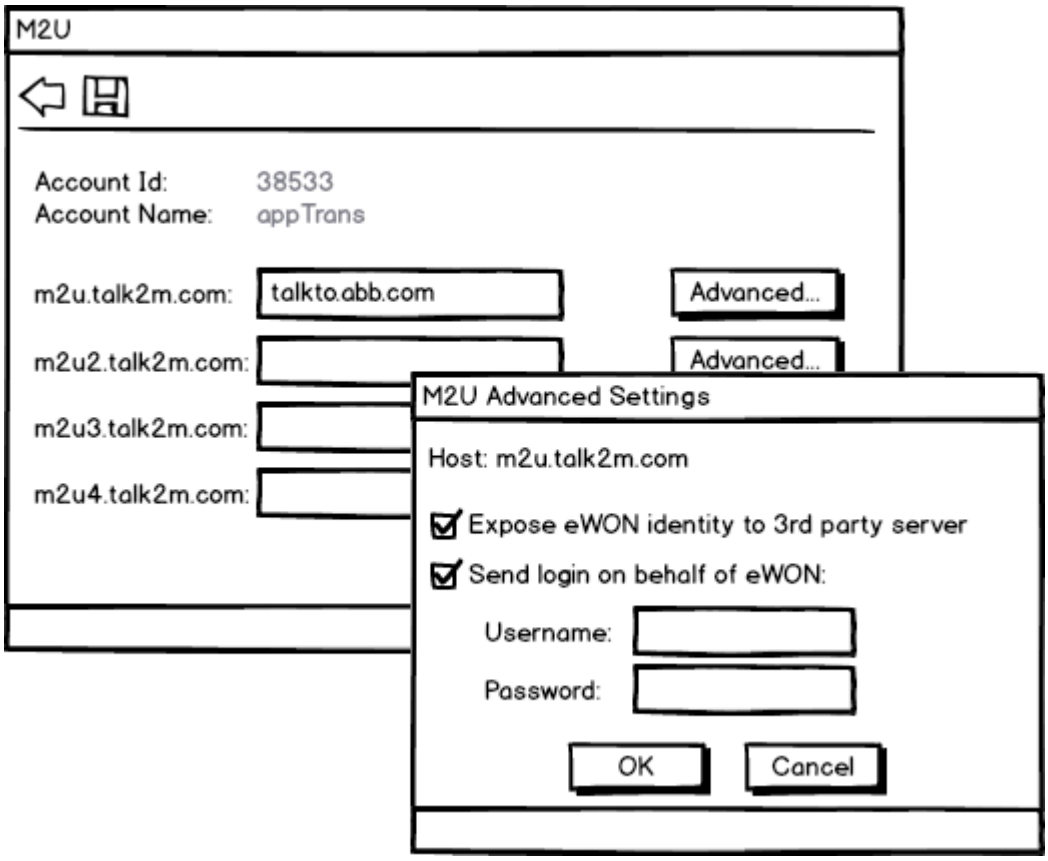
- Basic Authentication: In addition to letting the eWON use Basic authentication to connect the customer server, user can specify a centralized login in its Talk2M M2U settings. In this case, the Basic Authentication is performed by the M2U server rather than by the eWON. Note however that this is a per-account login. It does therefore not allow authentication of each single eWON since all eWONs in an account share the same login.

7. M2U Configuration

M2U is configured in eCatcher, in its own Account Details sub page (The M2U page is reached through the Account button in the vertical toolbar then the new M2U button in the Account Details toolbar.

NOTE: Prior to the official release of eCatcher4, beta testeres and early adopters should contact the Talk2M team to have their M2U config set on their behalf.

One can configure the server reached by M2U and optionally upload the client certificate that M2U should use when talking to this server.



Note that one is not limited to a single remote web server. eCatcher lets you configure several servers, each of which being reachable using its own T2M hostname: m2u.talk2m.com, m2u2, m2u3,...

The main goal to allow for several servers is to allow eWON users to subscribe to different services offered by various ESPs: One is not limited to one such service.