Secomea Security FAQ White Paper

Contents

Revision 1.5 – 2023-09-20

1. Chapter 1 - Web-Based security

For detailed knowledge on things described in this whitepaper and more, visit https://kb.secomea.com

Secomea Components:

1. **GateManager** (Access Management Server) - manages and facilitates encrypted connections between LinkManagers and SiteManagers
   - Support Go to Appliance (GTA) for WWW and in-browser VNC (remote access technology)
   - Support static device relays and server relays
   - Support log tunnels
2. **SiteManager** (IoT Gateway) - the hardware IOT device (or embedded software) typically installed along with a PLC/HMI or other industrial equipment that require remote access
3. **LinkManager** (Remote Access Client)- is the software/client used to gain secure remote access to industrial equipment connected to the SiteManager
4. **LinkManager Mobile** (Mobile Remote Access Client) - optimized for ease of access from a mobile device but can also be used on a PC for:
   - ○ accessing graphical interfaces of PLCs and HMIs
   - ○ operation, monitoring and helpdesk services

It is more restrictive by design (view only access) while implementing security principles from the LinkManager.

For detailed information on the solution the above form, check the following link: https://www.traceroutellc.com/blog-collection/secomea-comprehensive-secure-connectivity

The basics on remote security:

1. A Web-Client (your browser) does not know the specifics of a Webserver (conventional server), beforehand

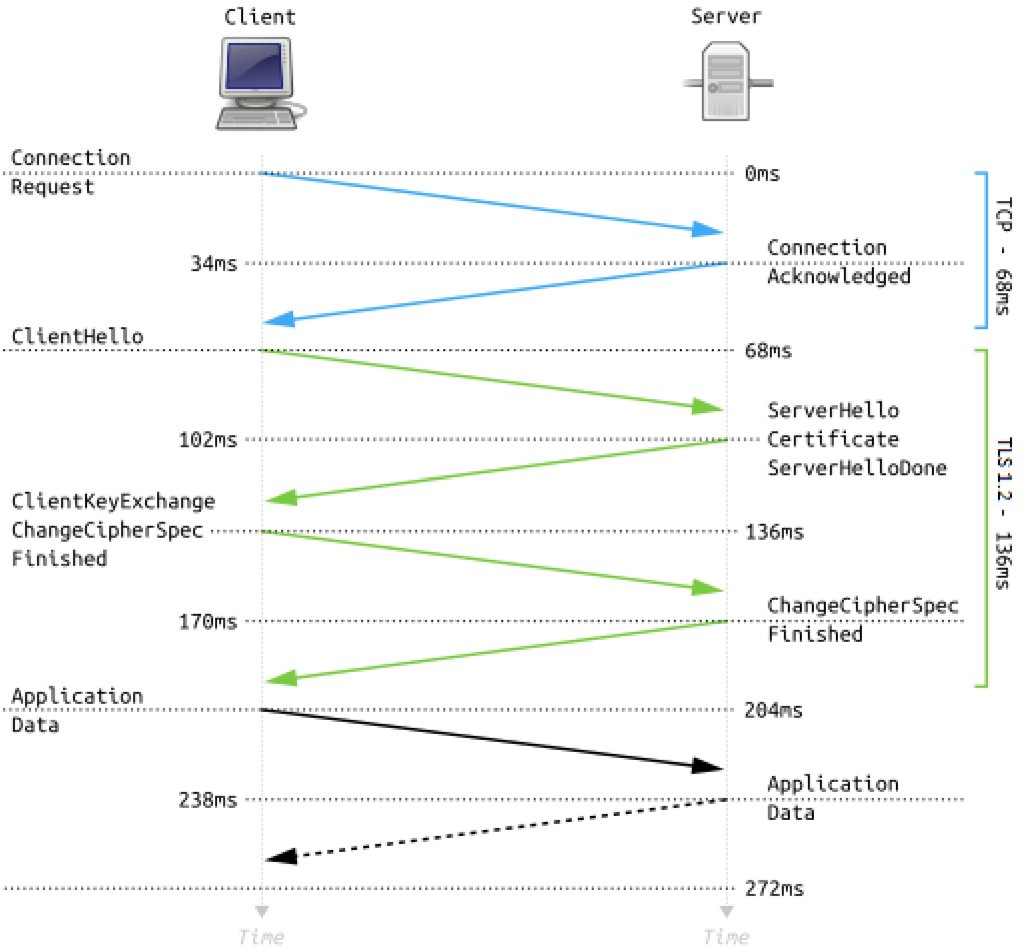
2. The two need to establish **trust** in each other, therefore:
   A secure version of the HTTP protocol called HTTPS used for communicating with the Webserver.
   HTTPS (Hyper Text Transfer Protocol Secure) appears in the URL when a website is secured by a TLS (aka SSL) certificate which provides:

   a. Confidentiality - A shared secret key does the symmetric encryption

   b. Integrity - A shared secret key does the message authentication code (MAC)

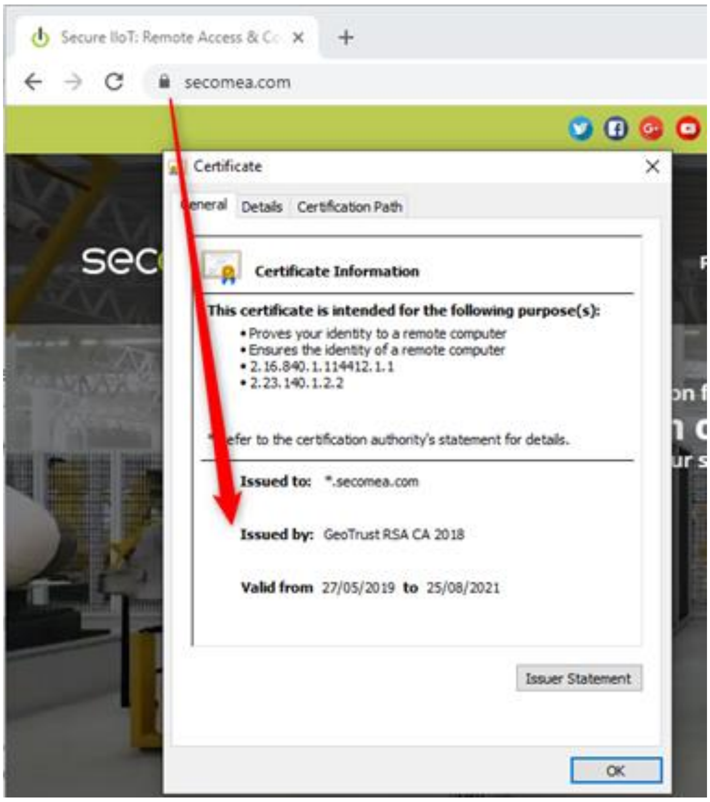
   c. Authenticity - Using certificate-based authentication leveraging the X.509 PKI standard (Public Key Infrastructure). Authenticates the client using a trusted CA (Certificate Authority) and the server during the TLS 1.2 handshake.

The above points use the **TLS 1.2 handshake protocol** displayed in the below image:



Examples:

Below is an example of the Secomea certificate, used at secomea.com. The certificate is issued by the GeoTrust CA (Certificate Authority), the browser then uses the Certificate to validate it with GeoTrust which will also help validate the contents displayed by the browser:



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.16.840.1.114412.1.1
- 2.23.140.1.2.2

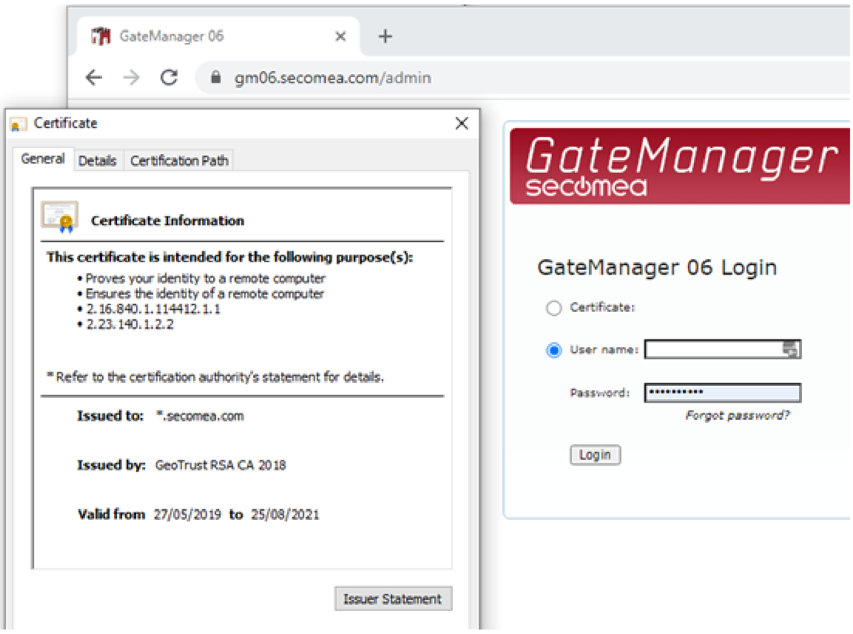
*Refer to the certification authority's statement for details.

Issued to: *.secomea.com

Issued by: GeoTrust RSA CA 2018

Valid from 27/05/2019 to 25/08/2021

The exact same process is used by the browser to validate the contents it displays received from the GateManager:



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.16.840.1.114412.1.1
- 2.23.140.1.2.2

*Refer to the certification authority's statement for details.

Issued to: *.secomea.com

Issued by: GeoTrust RSA CA 2018

Valid from 27/05/2019 to 25/08/2021

GateManager 06 Login

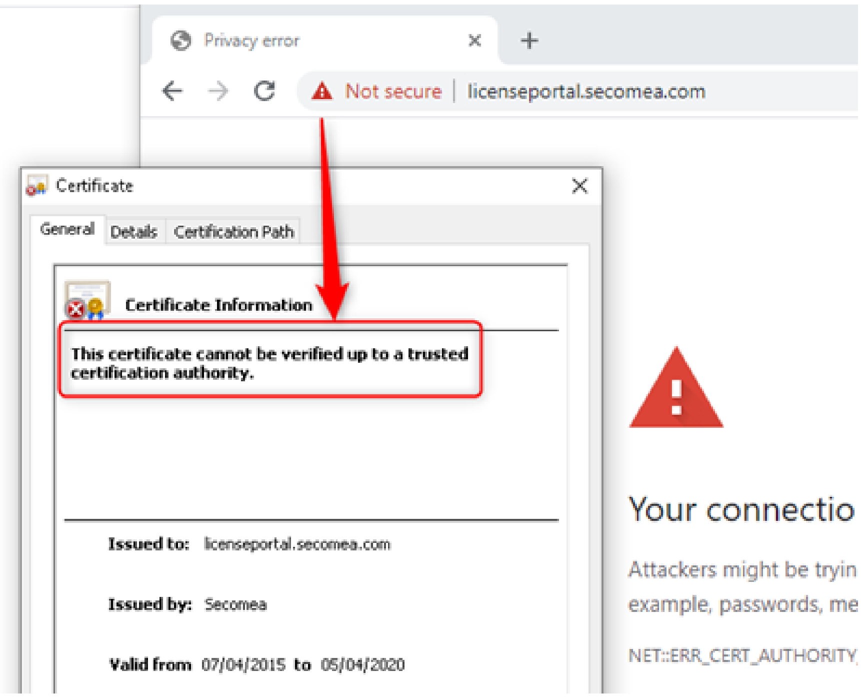
○ Certificate:

● User name:

Password: ••••••••••

Forgot password?

If the certificate cannot be verified with the CA (Certificate Authority), the browser will deem the certificate invalid, and alert the user with visual cues like the ones demonstrated below:



Not secure | licenseportal.secomea.com

Certificate

Certificate Information

This certificate cannot be verified up to a trusted certification authority.

Issued to: licenseportal.secomea.com

Issued by: Secomea

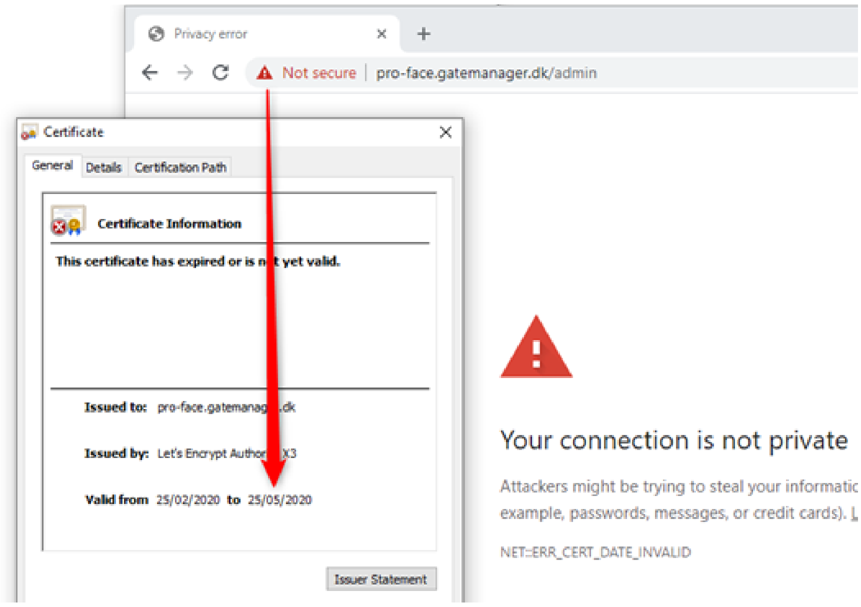
Valid from 07/04/2015 to 05/04/2020

Your connectio

Attackers might be tryin
example, passwords, me

NET::ERR_CERT_AUTHORITY_

The same alert will be displayed if the certificate has expired:



Not secure | pro-face.gatemanager.dk/admin

Certificate

Certificate Information

This certificate has expired or is not yet valid.

Issued to: pro-face.gatemanager.dk

Issued by: Let's Encrypt Authority X3

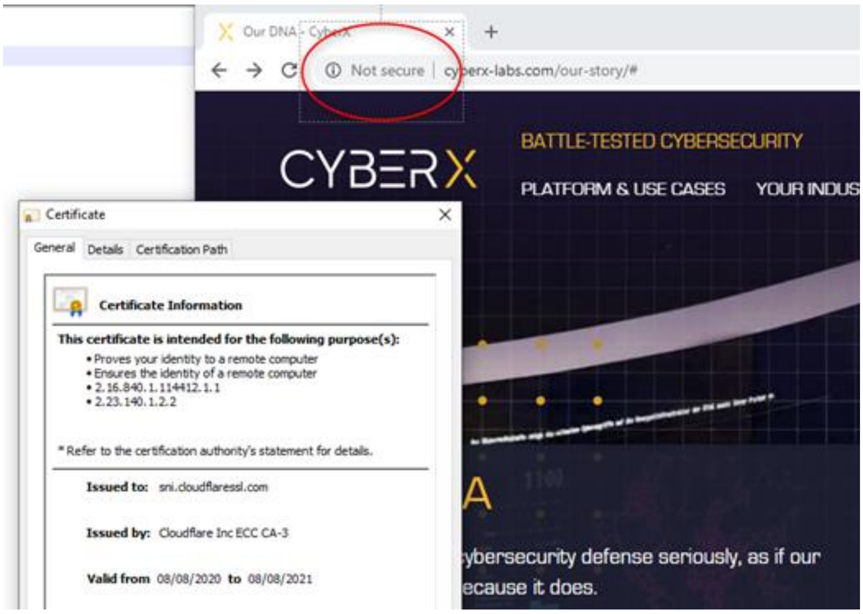
Valid from 25/02/2020 to 25/05/2020

Your connection is not private

Attackers might be trying to steal your informatic
example, passwords, messages, or credit cards). L

NET::ERR_CERT_DATE_INVALID

There are also cases where the certificate is valid, but the Webserver embeds elements of other sites that cannot be validated (which is a Cybersecurity risk), demonstrated on the below image:



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.16.840.1.114412.1.1
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

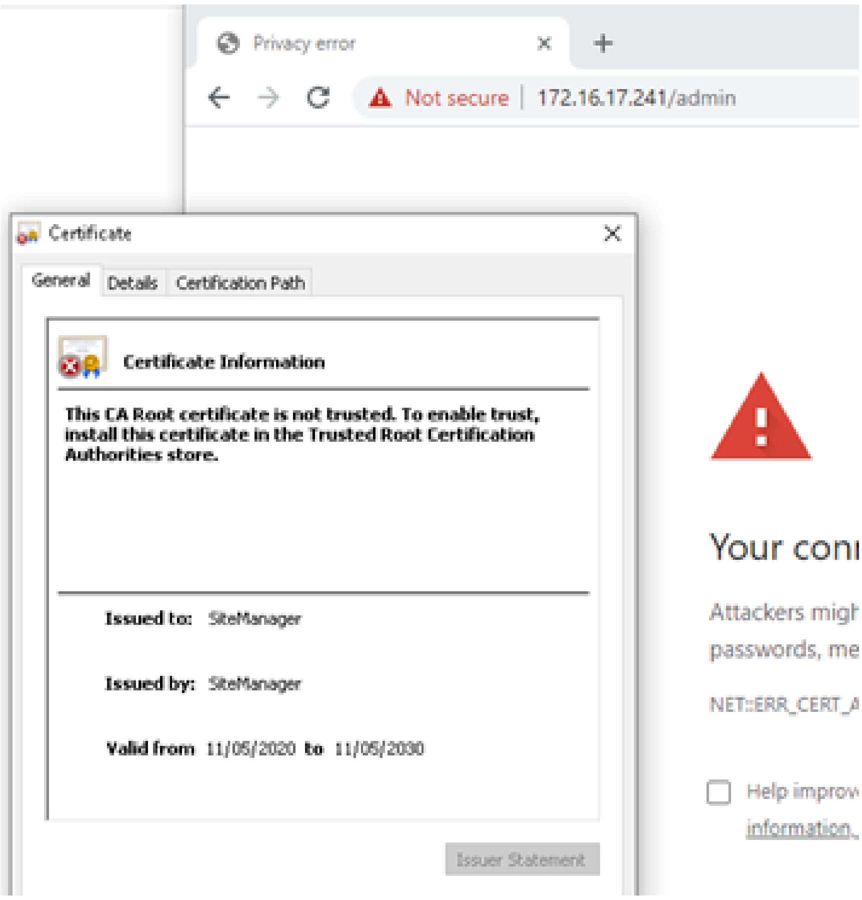
Issued to: sni.cloudflaressl.com

Issued by: Cloudflare Inc ECC CA-3

Valid from 08/08/2020 to 08/08/2021

How does our hardware module (Site Manager) use HTTPS:

The hardware SiteManager has an embedded HTTPS server for configuration. A SiteManager, however, does not have a DNS (Domain Name System) name associated with a CA that can authenticate. It only has an IP address, which is fixed or given by a local DHCP server. Therefore, a SiteManager will trigger the previously discussed browser security warning when attempting to connect to it locally:



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: SiteManager

Issued by: SiteManager

Valid from 11/05/2020 to 11/05/2030

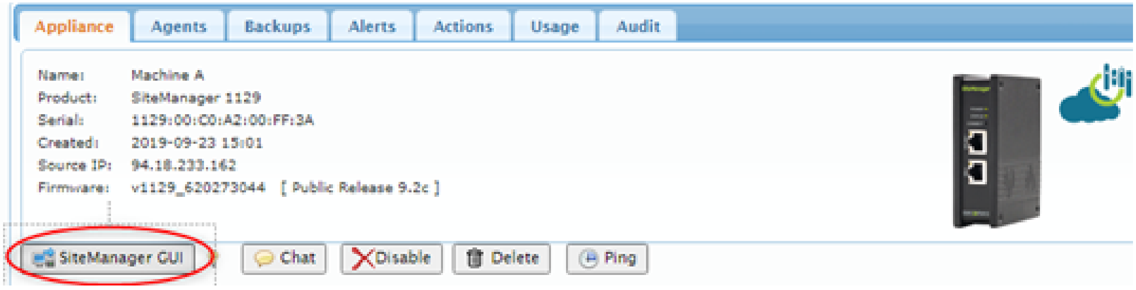
Your con

Attackers migh
passwords, me

NET::ERR_CERT_A

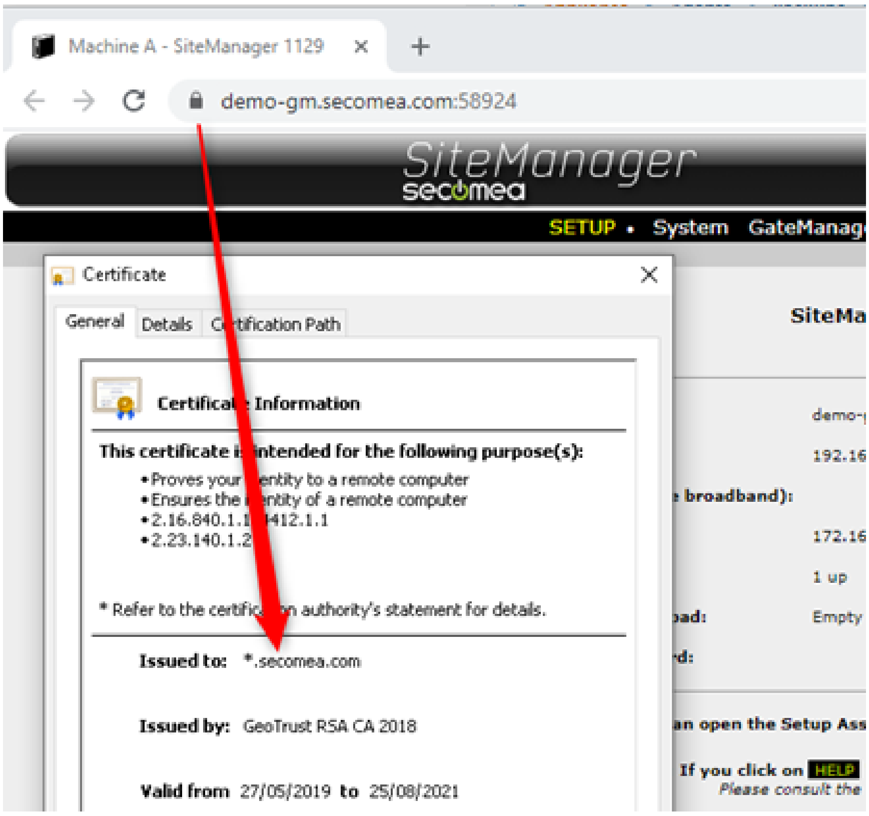
This applies to most internal network devices that use a web browser for configuration. Many devices (including PLCs and HMIs) still use plain HTTP, which will not trigger the certificate warning, but exposes clear text data on the network, while the SiteManager encrypts all the information it sends and receives. Often AD applied policies even restrict users from connecting to HTTP only servers.

However, in most cases, the SiteManager is configured (e.g., via a USB memory stick) to connect to the GateManager. Thus, all further configuration is done from the GateManager via a logged in administrator by clicking the "SiteManager GUI" button, which will ensure that the contents of what is displayed on the screen is accompanied by a certificate which has been validated as described in several sections above:



Name: Machine A
Product: SiteManager 1129
Serial: 1129:00:C0:A2:00:FF:3A
Created: 2019-09-23 15:01
Source IP: 94.18.233.162
Firmware: v1129_620273044 [Public Release 9.2c]

The HTTPS session will then be managed by the GateManager that your browser already trusts. Once we have come this far, you can securely browse pages on the web server, or login to services on the web server.



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.16.840.1.114412.1.1
- 2.23.140.1.2

* Refer to the certification authority's statement for details.

Issued to: *.secomea.com

Issued by: GeoTrust RSA CA 2018

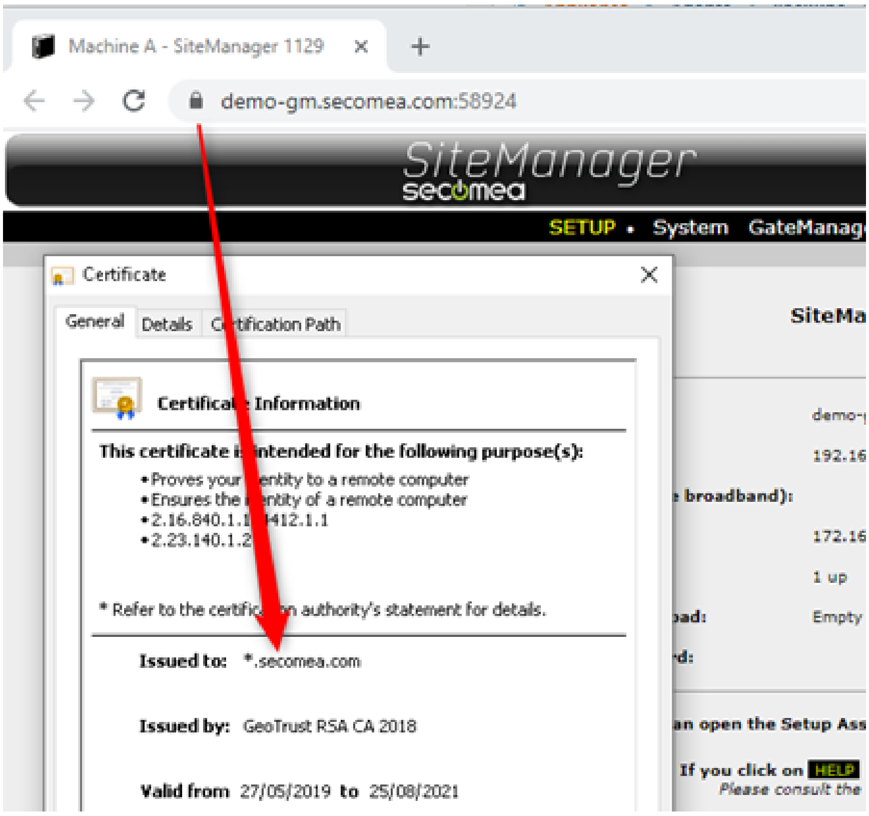
Valid from 27/05/2019 to 25/08/2021

2. Chapter 2 - LinkManager (Mobile) and SiteManager trust the GateManager

How is trust established?

The GateManager Trust Establishment

The GateManager is a HTTPS Web-Server, where all client access is browser-based.
As explained in Chapter 1, for any Webserver, you as a user, must be assured that you are connecting to the GateManager you already trust.
That is done by checking the DNS name and that your browser shows the Lock symbol indicating a CA validated certificate.



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.16.840.1.113412.1.1
- 2.23.140.1.2

* Refer to the certification authority's statement for details.

Issued to: *.secomea.com

Issued by: GeoTrust RSA CA 2018

Valid from 27/05/2019 to 25/08/2021

Once a secure TLS 1.2 (aka SSL) session is established, additional security is applied in the login process by:

1. Authentication - based on your credentials
2. Authorization - based on the privileges of your account (the account role and domains granted by the GateManager administrator)

The LinkManager Trust Establishment

The LinkManager Windows adapter is a passive component installed as a service on your machine and is fully controlled from your secure browser session with the GateManager server. A LinkManager does not have any connections to anything in idle mode. Connections are only initiated based on what your authorization grants you access to (see more details about LinkManager in a later section).

The LinkManager (Mobile) Trust Establishment

The LinkManager Mobile functionality has the same intent as the LinkManager; however it has been optimized to run on a mobile device and additionally provide a mobile friendly user interface. It uses the Gate Manager Web GUI / Certificate only + GTA.

The SiteManager Trust Establishment

A SiteManager is not a client, so how can it trust the GateManager?
In fact, you can consider a SiteManager a client. It just does not have a user controlling it.
It uses a slightly different mechanism to compensate for this, although the ground principles explained previously about TLS 1.2 are the same.

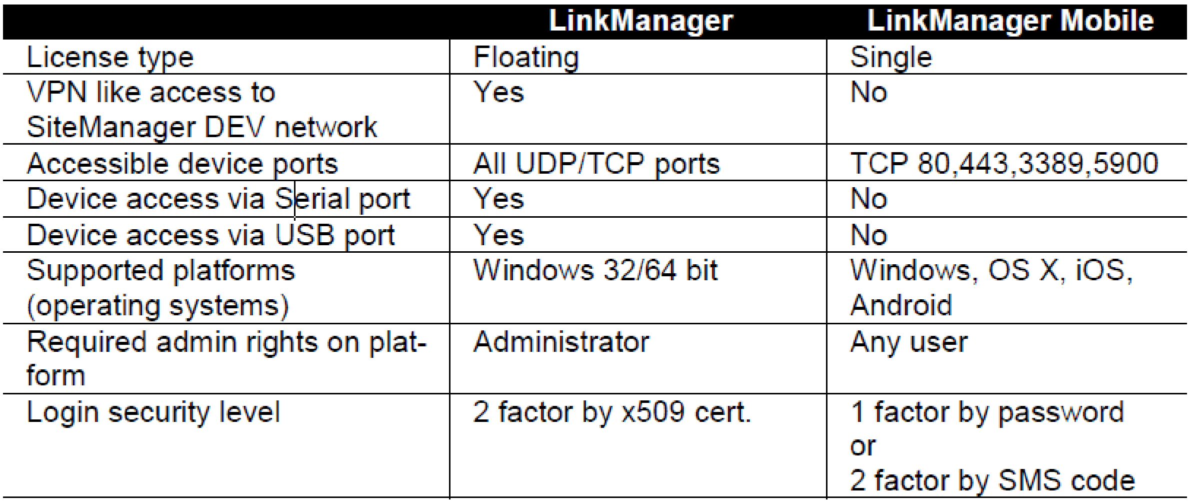
By default, a SiteManager has trust in any GateManager at the first TLS 1.2 connection. This is done by its preloaded public x.509 factory key issued by the same Secomea CA authority as the x.509 factory key on the GateManager. So, SiteManagers and GateManagers have trust in each other for the initial handshake.

This initial connection of a SiteManager is typically a manual portion of the SiteManager deployment, so the SiteManager should trust the GateManager that you have explicitly configured it to connect to, based on the entered GateManager IP address or DNS name.

However, the SiteManager still needs to ensure that it keeps communicating to the original GateManager and is not redirected to another server. Therefore, the first time the SiteManager connects with its factory certificate, it switches to using the unique TLS 1.2 certificate installed on the GateManager (following its license activation based on its DNS and serial-number). **This is similar to the browser scenario; however, the used certificate is issued by the Secomea CA (Certificate Authority), which is not issued by an external CA like GeoTrust.** This is due to the SiteManager not being able, as a web browser, to check the validity of the certificate at an external CA - as it is not allowed to connect to anything else on the Internet other than the GateManager. Therefor it simply binds itself to the unique activation certificate of the specific GateManager and will not accept connections to any other GateManager without that unique certificate.

Imagine your browser was locked to only connect to one single web server on the internet. To make the SiteManager connect to another GateManager, you must explicitly reconfigure the GateManager settings in the SiteManager, after which the certificate binding process starts over.

Quick comparison:



	LinkManager	LinkManager Mobile
License type	Floating	Single
VPN like access to SiteManager DEV network	Yes	No
Accessible device ports	All UDP/TCP ports	TCP 80,443,3389,5900
Device access via Serial port	Yes	No
Device access via USB port	Yes	No
Supported platforms (operating systems)	Windows 32/64 bit	Windows, OS X, iOS, Android
Required admin rights on plat-form	Administrator	Any user
Login security level	2 factor by x509 cert.	1 factor by password or 2 factor by SMS code

3. Chapter 3 - Where does the man-in-the-middle occur in all this?

The man-in-the-middle in this context is typically referred to as “phishing redirects.”

If an impostor takes over the identity of the original GateManager, by re-routing the connection, and simulates the GateManager IP address or DNS name, a successful connection will also require the unique TLS certificate of the server. Performing the last part is nearly impossible, as the certificate is bound to the unique serial number of the GateManager that is created at installation and used for license activation of that server.

4. Chapter 4 - How does the GateManager trust the SiteManager?

For this chapter we must introduce the definition of an Agent: An agent is something that you configure in a SiteManager for computers (LinkManager) to communicate with specific end devices on specific ports (more granular than IPs). They contain functionality and knowledge about the device that is connected.

The previously explained measure was primarily to protect the SiteManager from a hostile Server. So, how to protect the Server from a hostile SiteManager "Client" which you cannot validate by login authentication as you can for a user with a browser.

By design, and for ease of deployment, you configure a SiteManager to connect to any GateManager publicly available on the internet and to a domain that exists on that GateManager, e.g., ROOT.AcmeInc. If that domain exists, the SiteManager will connect and attach in that domain.

Since a SiteManager is a passive component, it cannot, by just connecting, send harmful data to the GateManager or its users, nor can it extract any information from the GateManager. To access data of any kind, a LinkManager must explicitly connect to a specific SiteManager or an agent on the SiteManager.

If an adversary had intentionally directed a SiteManager towards your GateManager, your LinkManager users should still be authorized to connect to it, with good reason. If the villain's purpose is to attack the LinkManager Client, then the SiteManager would have to be connected locally at the villain's network to some infected server, represented by a configured agent.

GateManager administrators monitor their domains and would be suspicious of SiteManagers appearing for an unknown reason. You can also specify on the GateManager a security level which requires all SiteManagers attempting to connect to be explicitly attached to a domain by the GateManager administrator.

In fact, SiteManager Embedded (SM-E) always must be bound manually to a domain as part of the license assignment process. It is doubtful that anyone would assign an activation license to an unknown SM-E.

5. Chapter 5 - Is a LinkManager Windows adapter vulnerable to malicious connections?

This is a good question, and of course something that has been key to the design.

Firstly, a LinkManager connection always requires activation through a GateManager authentication and authorization process. The GateManager simply will not accept a LinkManager connection if it has not been explicitly allowed, following:

- A LinkManager client login authentication
- Authorization
- The connection attempt to a SiteManager Agent

The LinkManager Windows adapter will additionally prompt the LinkManager user on the local PC, for authorization to use this GateManager or LinkManager account with the LinkManager adapter.

Once authorized, and the LinkManager adapter has established an encrypted connection to the GateManager, the ports specified by the SiteManager Agent at the remote end are accessible by any application on the Windows user's PC.

Link Manager Login Security Levels:

- SSO with authenticator
- MFA with certificate + password + SMS
- Username/password (also available for Link Manager Mobile with optional MFA by SMS)

6. Chapter 6 – Using unencrypted protocols towards the end-device

The LinkManager adapter simply forwards all traffic "as is" between the local PC and the endpoint of the remote device, i.e., if the remote service is not encrypted, the traffic (internally to the LinkManager PC) is not encrypted either. Only the destination IP's and ports explicitly opened according to a specific agent type will forward traffic. I.e. traffic not destined for a specific agent (IP/port) will not be forwarded from the Link Manager to the Site Manager side.

In this way, it is just like any other VPN tunnel service that you can operate on a PC. For example, if you had used Cisco AnyConnect to a remote network and accessed a PLC (Programmable Logic Controller) web server using the HTTP protocol, the traffic - internal to the PC - would also be (unencrypted) HTTP. Still, for both LinkManager and AnyConnect, the traffic forwarded outside of the PC (between the PC and the remote VPN endpoint - SiteManager or AnyConnect server) is fully encrypted.

7. Chapter 7 - How to avoid getting components hacked on their public IP addresses?

GateManager and LinkManager user accounts, given they are based on a web browser, are always located behind firewalls, typically both a corporate one and the personal firewall on your PC.

As mentioned, the SiteManager essentially works as a web client, meaning that all traffic is outbound on port 443. SiteManagers typically are connected to a local intranet and therefore connect via the local internet firewall. When remote access is initiated, it is done via the encrypted outgoing connection established with the GateManager. Even if a SiteManager is connected directly to the internet via a 4G connection, there are no open ports on the SiteManager, and nothing that a hacker can work with (In fact, a 4G version of a SiteManager does not require any special subscription, and does NOT as some other solutions, require a SIM with a fixed IP address).

The GateManager is also located behind a suitable firewall, and like a typical web server, the only port the firewall requires to forward from the outside to the GateManager is port 443, for the previously described TLS 1.2 handshake from GateManager and LinkManager Clients and SiteManagers to work.

The Secomea cloud based GateManagers are all behind monitored firewalls, and should you choose to migrate to a GateManager Own it would be protected against attacks by your corporate security system.

Unlike most other remote access solutions, the Secomea solution is not relying on the internet. You could deploy the GateManager and subsequently clients and SiteManagers, in a totally closed WAN network. If granting access for remote access users from outside the WAN, you could apply a second layer of authentication (such as an RSA token) to access the WAN before the user can access the GateManager and through this be authorized to access remote devices via SiteManagers.

8. Chapter 8 – Can a hacker exploit Gate Managers access to end devices?

The GateManager does not hold any persistent connections to any end-device. It only holds service connections with the SiteManagers to check status and for fleet management purposes (firmware upgrade, configuration etc.).

Only when a LinkManager connection is requested by an authenticated and authorized user, will the GateManager open a proxy connection to the ports of the relevant SiteManager agents representing the service endpoints of the remote devices. Such proxy connection is end-to-end encrypted from the LinkManager to the SiteManager, so no other services or programs on the GateManager peek into or utilize this connection. The GateManager simply proxies the encrypted connection.

9. Chapter 9 - Secomea supports two factor authentication. Is this the x.509 certificate used?

Two factor authentication, typically referred to as 2FA, means a second layer of authentication and the two factors must be at least two of the following: Something you know (e.g., a password), something you have (e.g., a smartcard), something you are (e.g., biometrics), or something you do (e.g. voice).

The Secomea solution historically used x.509 certificates for client login. Today a secure token in the form of an encrypted digital file is used instead, although it is still referred to as a certificate. X.509 certificates are still used both in the TLS 1.2 handshake process, and for SiteManager connections.

When using a digital certificate as a second factor, it is assumed it is stored on a piece of hardware that only you are in possession of. This, in combination with the password that only you should know, constitutes 2FA.

Some argue, with good reason, that since the certificate is not tied to the physical hardware (the PC), then it cannot be considered the second factor, i.e. you can load the certificate on several PCs.

Secomea integrated this by design to increase flexibility, but admittedly it is not textbook 2FA. However, an optional feature on the GateManager allows you to lock a specific LinkManager to a specific PC, so if the certificate were copied to another PC, the GateManager would reject it despite the correct certificate.

To obtain an additional layer of authentication, you can enable SMS on the GateManager as an additional factor. In this case your phone represents the additional factor, i.e. the hardware that only you have in possession.

If you further combine this with the certificate, i.e. password + certificate + SMS, then we could argue for 2½ factor authentication.

10. Chapter 10 - How does LDAPS and AD, Azure AD fit in?

By default, the authentication and authorization process are self-contained in the GateManager. That means users must be created and administered in the GateManager portal. Many find this convenient as users may be external to the organization, and should not be managed by the corporate AD.

When talking AD (Active Directory) or LDAPS (Lightweight Directory Access Protocol), we refer to managing authentication external to the application or service. That is, the login validation is done by the GateManager against a central user database that also controls access to other applications and services. The advantage is that when an employee leaves the company or should have privileges revoked or extended, it is done in the central user database, without having to engage the GateManager.

Often the user database, in addition to user identification, also holds the policies for a specific application. This could be the user’s authorization, such as their role in the application, and/or what rights the user has. In a GateManager context, LDAPS authorization might be the user’s classification as a LinkManager or Domain administrator, and what Domains they have access to.

The GateManager has an optional JSON API (Application Programming Interface) for controlling both user authentication and authorization externally. This is called CRM API and is available on own GateManagers.

GateManager is also capable of authenticating users using LDAPS (e.g., against an MS AD Server). We also support OpenID Connect which natively matches a user to a Microsoft Azure account.

11. Chapter 11 - How does “Zero-trust” apply to the Secomea solution?

Zero-trust has many definitions depending on context, but the most relevant here is:

- “No security difference between Intranet and Internet” - This means that the Private Network cannot be trusted, meaning that Virtual Private Networks (VPN) cannot be trusted either.

One element of zero trust is that all communication to all endpoints must be secured, and verification is required for everyone trying to get access to resources on the network. Further, you no longer rely on internal "perimeters" (Intranet), which are usually trusted.

Here are only some of the measures that have been built in to adapt Secomea to a zero-trust context:

- The option to allow no external access to the SiteManager access gateway itself. It can solely be controlled by the local OT (Operation Technology) onsite, and central control by the GateManager administrator is removed
- Ability to deploy the GateManager as part of the internal OT/IT controlled infrastructure, and not as an external Cloud service
- Fine-grained access authorization - a user can access only specific end-devices, and only certain ports on the end-device
- Device access can be made in timeslots, or authorized by the operator locally (e.g. controlled by an input port on the SiteManager)
- All access activity is logged for auditing but can also be made available for real-time monitoring so suspicious activity can be intervened
- Ability to deploy the SiteManager as a software component directly on the end-device, and thereby eliminate potential unencrypted industrial protocols being exposed on the network

The above measure ensured that the Secomea solution is designed with the below facts in mind:

- Since the Secomea solution is designed to facilitate UDP/TCP real-time connections, it cannot by itself fulfill requirements for verification to specific endpoints, simply because it does not know if for example, a technician connecting from a PLC application to a physical PLC is allowed to do so
- It also cannot control a potential native login process between the technician's application and the PLC
- Neither can the Secomea solution ensure that the local communication between the SiteManager and the PLC is encrypted

12. Chapter 12 - What extra security can be applied on top of the solution?

Different measures can be applied, but it really depends on the context and scenarios you want to address. Measures may increase control, restrict actions or access, but they may also reduce usability, so often there are trade-offs. Examples of security elevation initiatives:

1. In your security system (firewall): restrict the SiteManager to only access the GateManager (source/destination rule).
2. Direct the real-time logging of the GateManager to a central syslog server such as SPLUNK and apply measures to identify cyberattacks.

3. Some of the measures are mentioned earlier, such as enforcing 2FA, requiring explicit approval of all new SiteManagers and restricting LinkManager access to specific PCs by using the GateManager feature of locking the LinkManager instance to a PC controlled by IT policies.

Some of these topics are described in more detail on our online Knowledge Base; otherwise, our support team is available to discuss specific concerns.

13. Chapter 13 - How to prepare against new hacking techniques?

Any IoT solution can be subject to attacks. And any IoT solution will, at some point in time, be subject to vulnerabilities; either by discovery of vulnerabilities in components or because of the way the solution is used. A vulnerability does not necessarily mean you will get attacks, and most vulnerabilities are discovered before hackers exploit them.

So, the trick is to fix or mitigate vulnerabilities before they become a problem to your business.

The Secomea solution is subject to regular security audits, which include penetration testing by external security experts. But even experienced security specialists cannot discover all potential vulnerabilities. To address this, Secomea has developed a Cybersecurity Advisory process, allowing anyone to report a vulnerability. Subsequently Secomea assesses the report, and if it is indeed a vulnerability, Secomea releases fixes with instructions on how to mitigate.

The findings, with fixes and mitigations, will be disclosed by CVE (Common Vulnerability Exposure) reports, so that the information is available in public CVE databases that you can subscribe to. Even vulnerabilities discovered internally in our testing and own audits will be disclosed as CVEs (Common Vulnerability Exposure), so that the information is made available to the OT/IT departments of our customers.

14. Chapter 14 – Traditional-VPN vs Relay-VPN

We kept our most frequently asked question for last 😊

Earlier generations of Secomea remote access also used traditional VPN, but our third-generation secure connection method introduced in 2010 is based on tunneling traffic via a proxy connection, rather than routing connections. We call it "RelayVPN" to highlight that it has the same end-to-end connection capabilities as traditional VPN.

RelayVPN is based on TLS 1.2 connections based on x.509 (1024-bit keys) and AES256 encryption, just like SSL VPN (used by e.g. OpenVPN). So, security wise, in terms of key exchange and encryption, the Secomea solution and OpenVPN are remarkably similar.

Both OpenVPN and RelayVPN transparently carry Layer3 traffic (UDP and TCP), and even Layer2 if appropriately implemented by network adapters on both ends (although not all OpenVPN solutions would support Layer2).

Proxying connections have the advantage of eliminating potential issues of IP or subnet conflicts. Such challenges are typically handled by routed connections using NAT. However, handling overly complex network scenarios is exceedingly difficult to accomplish with NAT and security system rules alone. Secomea's RelayVPN eliminates most of the NAT issues one might have in many-to-many scenarios typical for industrial remote access. Additionally, Relay VPN addresses the multidimensional access need for fine-grained differentiated user access at device and port level.