MyMilli-Q™ Remote Care NETWORK SAFETY DATASHEET Rev 6.0

The Life Science Business
of Merck operates as
MilliporeSigma in the US
and Canada

Contents

Milli-Q®

Lab Water Solutions

Network topology

Your Milli-Q® water system can be connected to any network via an Ethernet plug.

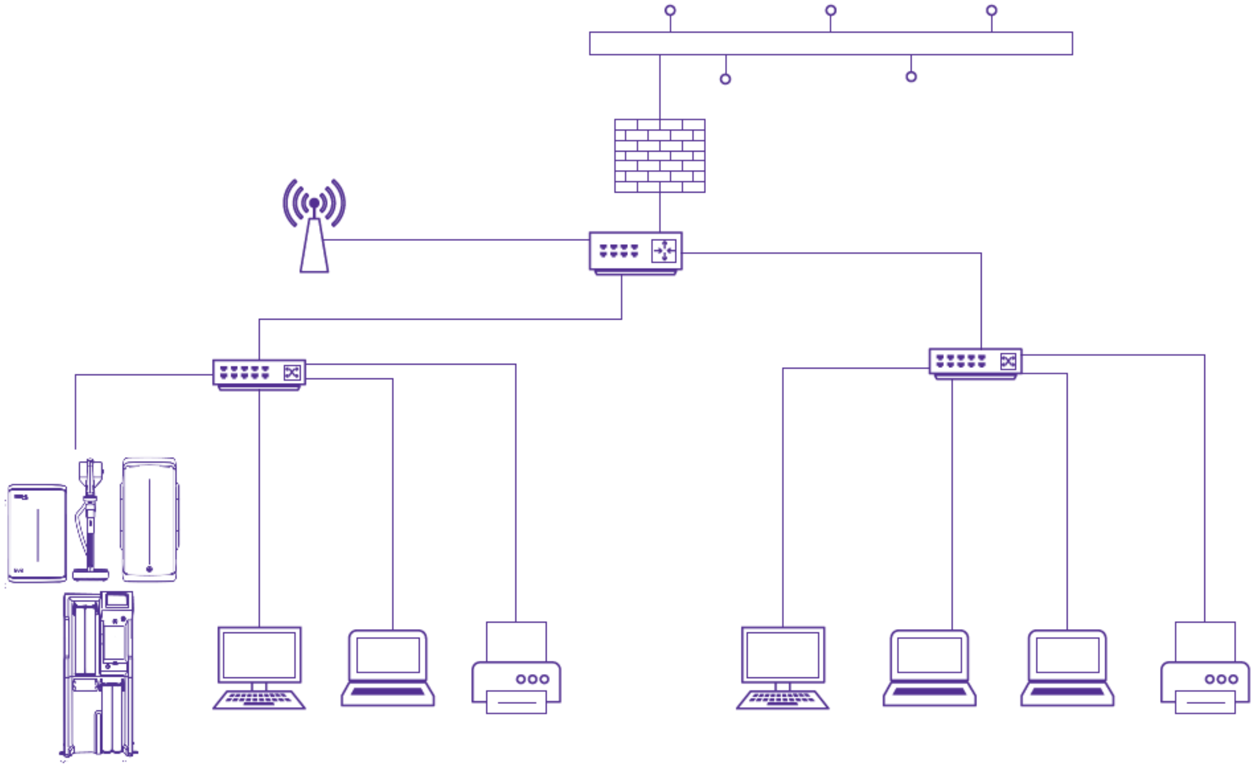


Figure 1: Example of network topology

Network configuration

The Milli-Q® water system is only compatible with IPV4.

IPV6 is not currently supported but may in the future be delivered by a software update.

The Milli-Q® water system can be configured as a DHCP client and therefore be assigned a network configuration automatically, or it may be configured manually with a static IP address, subnet mask and gateway address. DHCP client is the recommended mode as the configuration is easier to manage and maintain.

Local services

The network connectivity of the Milli-Q® water system gives access to services available directly on the local network by using the IP address of the Milli-Q® water system. For these services, the Milli-Q® water system acts as a server.

There are only 3 TCP ports (and 3 services) on the water purification system which can be accessed from outside:

- Port 80 (http): Only redirects to the more secure port 443 (https)
- Port 443 (https): Allows access via a web browser to the touchscreen interface of the system
- Port 22 (ssh): Allows specific console access for Merck R&D services or the Merck manufacturing plant (secured by an RSA 2048-bit private key)

All other incoming connections will be refused by the firewall embedded inside the water system.

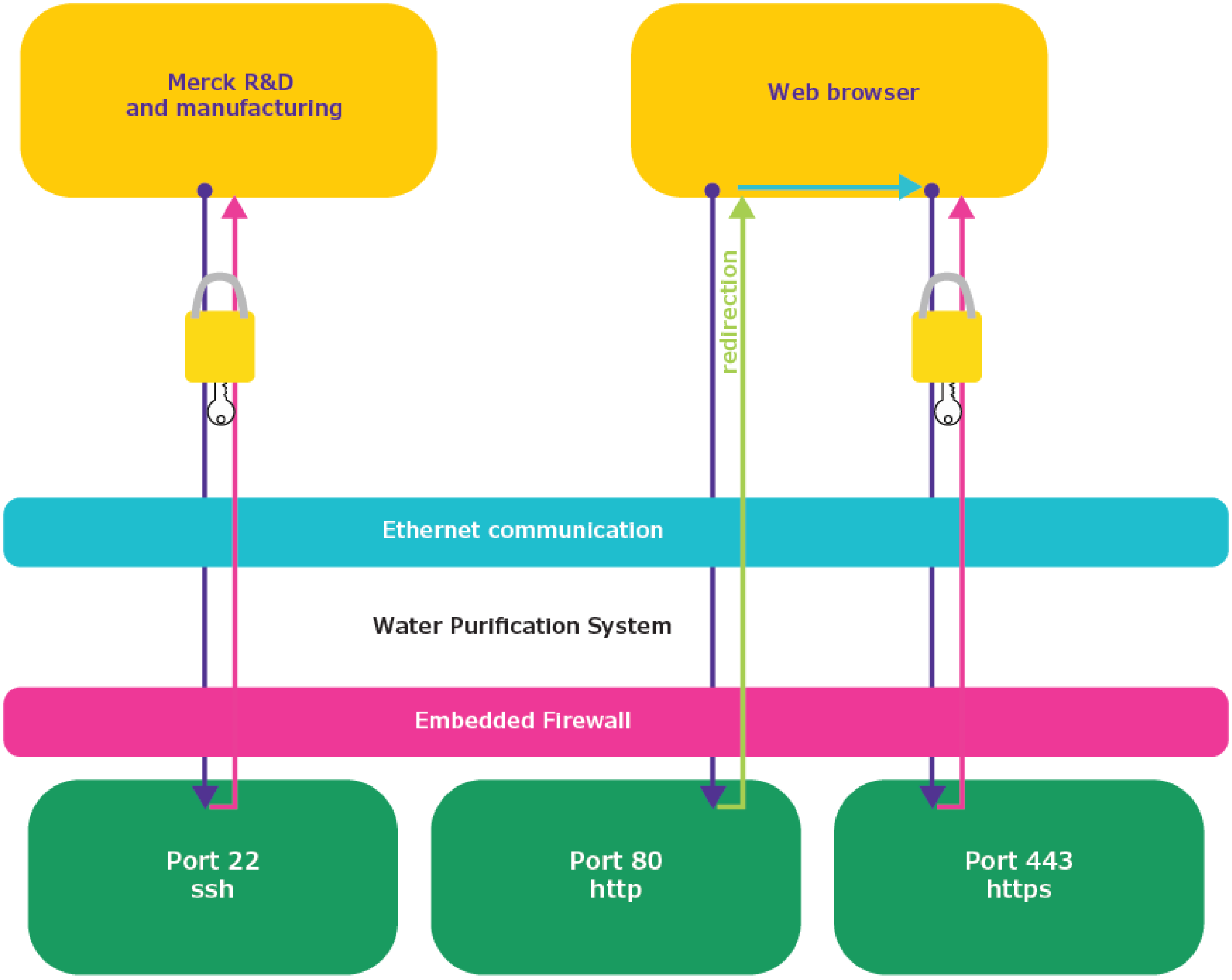


Figure 2: Local services

Cloud services & data

System monitoring

The water purification system can be configured to connect to the Merck cloud to push specific data regarding the status of the water purification system. This data is available to both the customer, for monitoring and traceability of their system's performance, as well as to Merck, to improve the quality and reactivity of the provided care.

If the embedded MyMilli-Q™ Remote Care agent has been enabled in the system, it will attempt to connect to the Merck cloud using the configured gateway in order to push the following information:

- Alarms/alerts as they occur
- Daily measurements and operational statistics at the end of the day
- Certain configuration parameters, only when this type of information is requested by a user or a service
- Consumable status information, only when this type of information is requested by a user or a service

Remote control

Our service engineers can connect remotely to the water purification system and perform a remote diagnostic as if they were in front of the system. This remote connection passes through a secure and encrypted communication tunnel. For safety reasons, a user in front of the system must grant access to the remote service engineer using the Milli-Q® water system's touchscreen. The user can interrupt the remote session at any time. The session cannot exceed 1 hour. The secure tunnel is established and remains open exclusively for the duration of the session. Our service engineers are the only ones able to connect remotely to Milli-Q® water systems and are authenticated by the Merck network.

Milli-Q® water purification system outgoing connections

The only outgoing connection attempts that may be executed by Milli-Q® water systems are the following:

- Request IP address allocation to a DHCP server (uses UDP on port 67)
- Request domain name resolution to a DNS server (uses UDP on port 53)
- Connect to the Remote Care service of the Merck cloud (uses TCP on port 443 at address https://api.mymilliq.com).

Embedded security technologies

SSH connectivity

Milli-Q® water systems embeds an SSH server to allow secure console access. This access is strictly reserved for Merck R&D and manufacturing services. The embedded SSH server has been proven to be highly secure and it is configured to authorize connections only from Merck R&D and manufacturing entities who are the only ones to own the RSA 2048-bit private key. Password authentication through SSH has been disabled to improve security level of this access. This access is not accessible remotely.

HTTPS connectivity

If you are unfamiliar with this technology, refer to Annex 1 for an introduction.

The https connection uses TLS 1.2 and AES 128 bits.

Local services

Any connection issued from a client (typically a web browser) to the local ports 80 or 443 of the system will initiate a secure https connection. Depending on the browser, a warning message can appear because the certificate is not signed by a Certificate Authority. This is not possible because the IP address of the water purification system is not predictable and depends on the customer’s network. The warning has no impact on the level of security and the entire communication is still encrypted.

Cloud services

When the Remote Care agent is enabled, any connection issued from the Milli-Q® water system to the cloud is performed on port 443 of the cloud server. Every Milli-Q® water system has its own certificate which uniquely identifies it. The cloud platform also has a certificate that ensures its own authenticity. When communication is initiated, each component verifies the other’s identity by checking the contents of the other’s certificate. Once mutual authentication has been performed, the entire communication is encrypted.

The Milli-Q® water system connects to the cloud server at the following URL: https://api.mymilliq.com.

Embedded firewall

The embedded firewall has been configured with the following rules:

- Any incoming connection that is not directed to the authorized ports (UDP 68: DHCP, TCP 22: SSH, TCP 80: HTTP and TCP 443: HTTPS) will be ignored.
- Any outgoing connection that has not been initiated by the authorized ports (UDP 53: DNS, TCP 443: HTTPS) will be blocked.
- ICMP protocol has been authorized to make ping request available.

Remote control

Secure Websocket technology over TLS protocol – mutual authentication (Server and client) with 2 factors.

OpenSSL credits

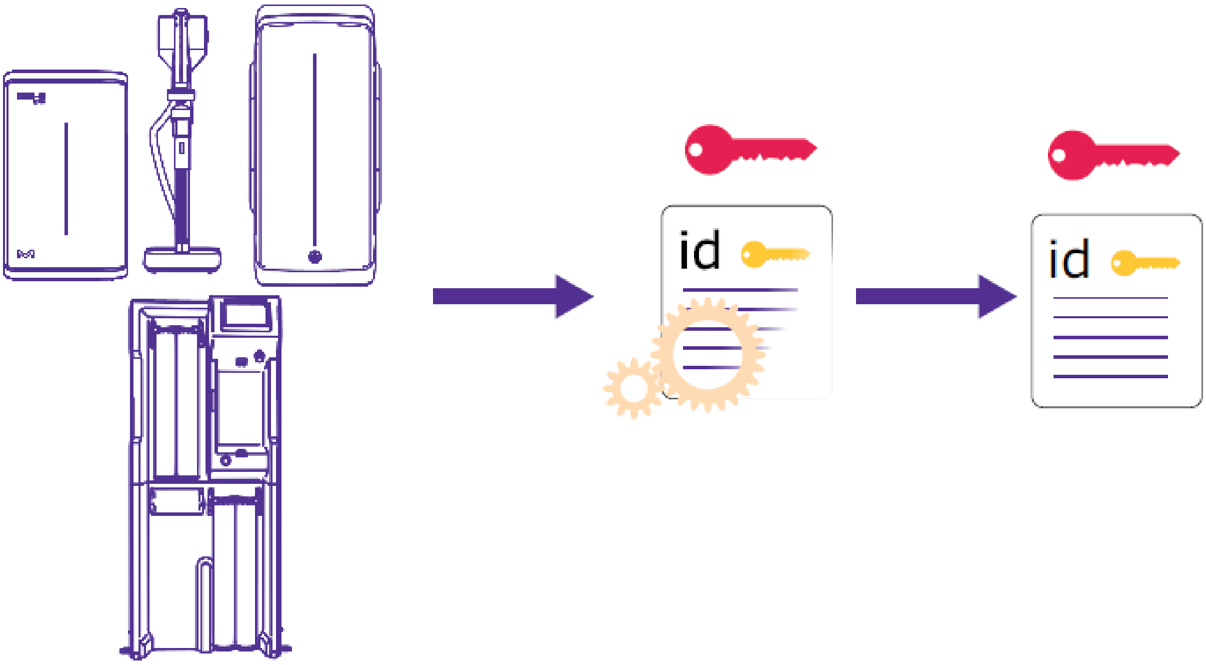
This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

Annex 1 : Introduction to TSL 1.2 in Milli-Q® water purification systems

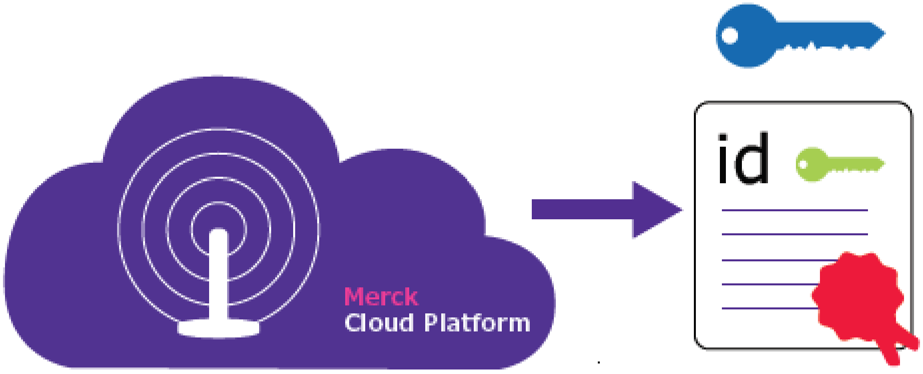
Security: mutual authentication & communication encryption

Register and authorize the Milli-Q® water system

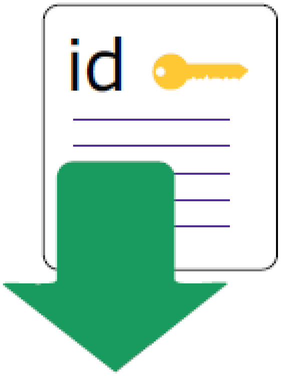
1. The Milli-Q® water system generates a private key and a certificate containing its unique id and the corresponding public key.



2. Our internal cloud platform also has its own private key and certificate already approved by a well-known external certification authority.

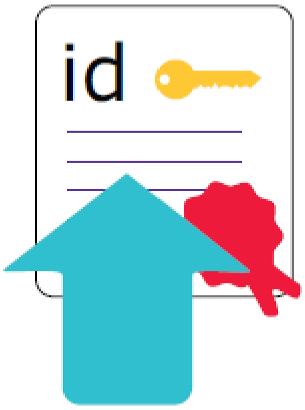


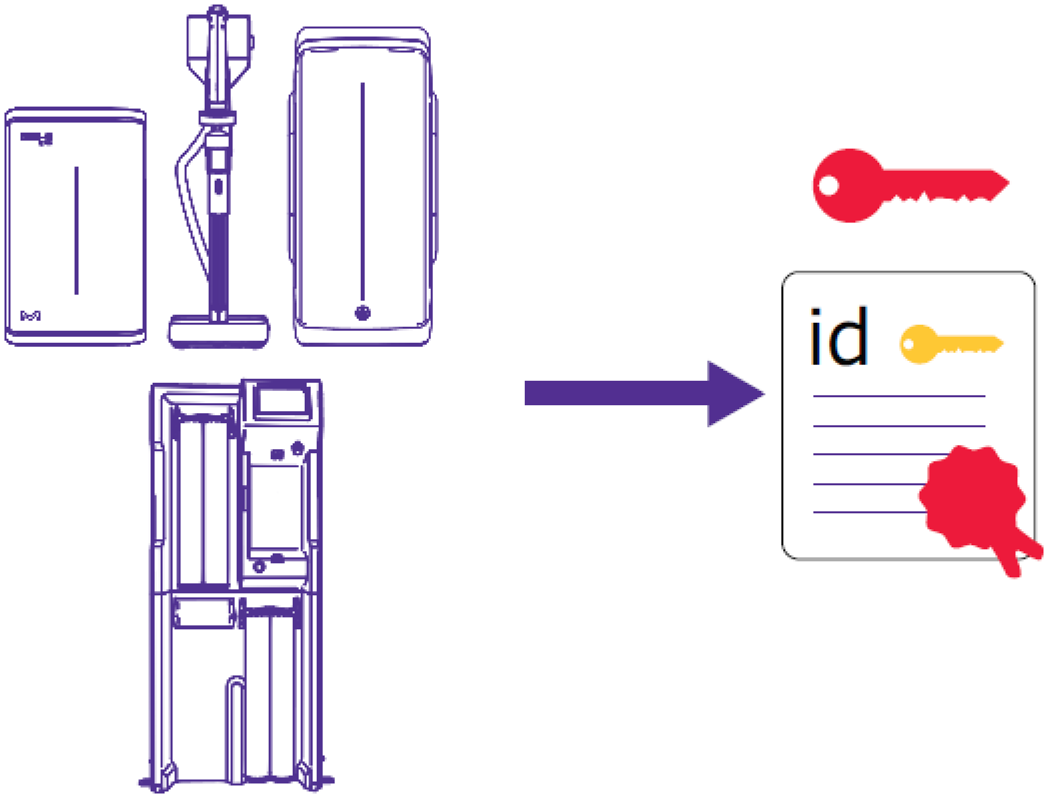
3. The service engineer who installs the Milli-Q® water system in the lab downloads the certificate, which uniquely identifies the Milli-Q® water system.



4. By using service tools, the service engineer requests our internal cloud platform to authorize and sign the Milli-Q® water system's certificate with its private key acting as a certificate authority.

5. He then uploads the signed certificate back into the Milli-Q® water system.

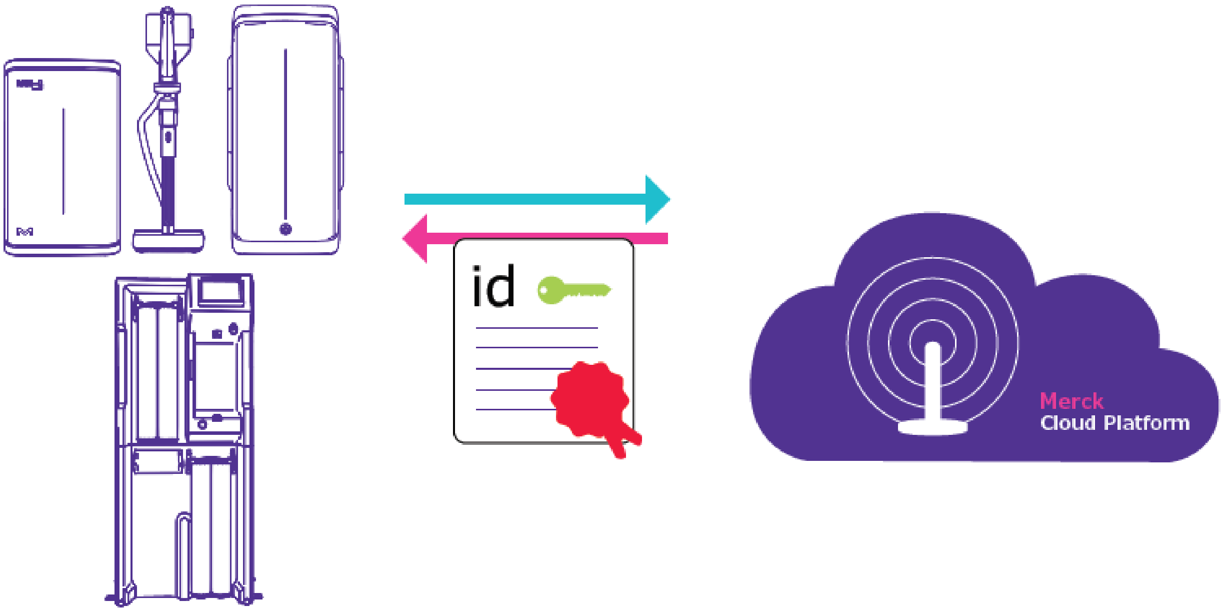




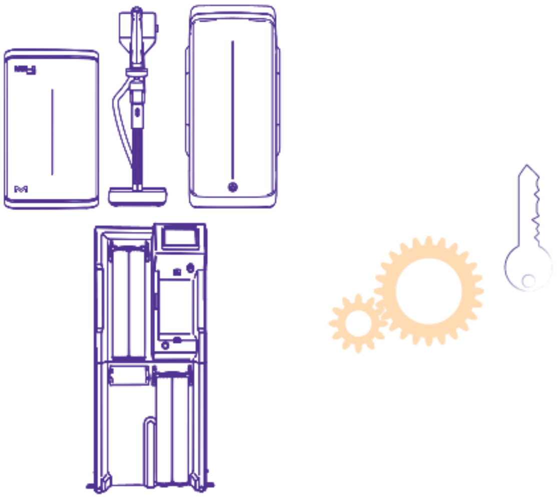
Now the water purification system has a private key and a signed certificate to prove its identity when it connects to our internal cloud platform.

Connect and communicate securely

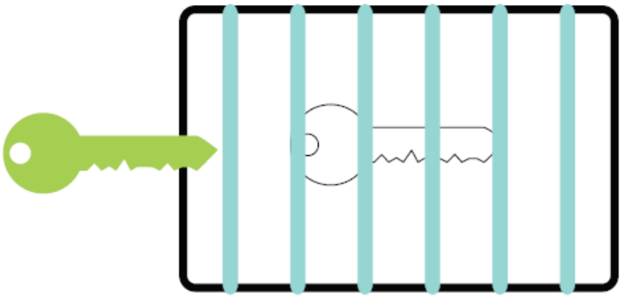
1. When the Milli-Q® water system tries to connect to the Merck cloud platform it first receives the platform's certificate. By using the included public key, the system can verify that it is really connecting to the platform and not something which is trying to usurp the identity of the server.



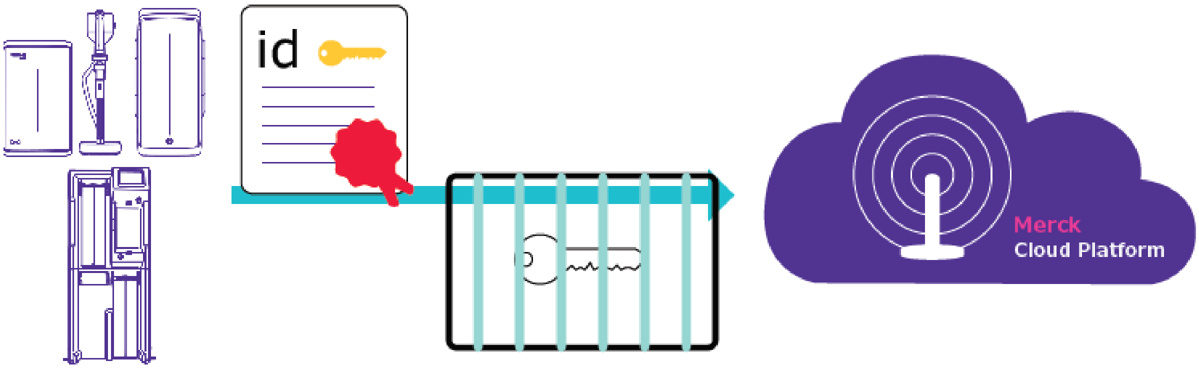
2. The Milli-Q® water system then generates a session key which will be used to encrypt the entire communication.

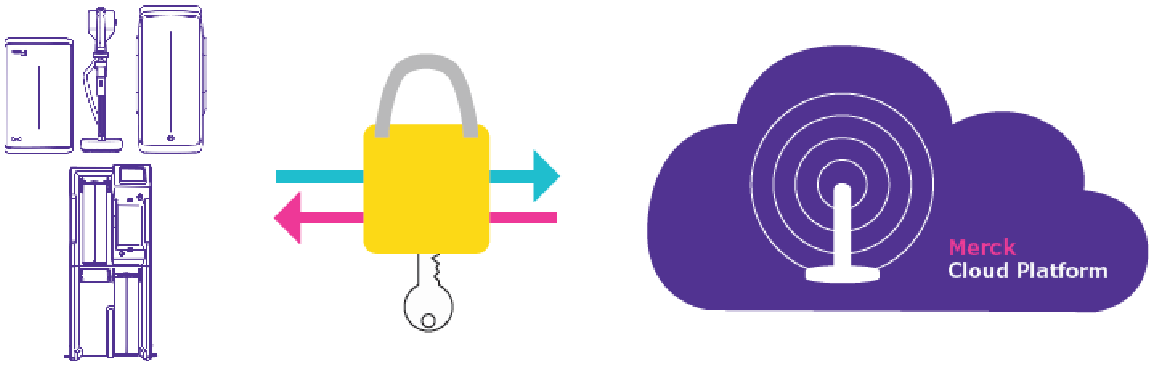


3. By using the Merck cloud platform public key, the system can encrypt the session key so that only the Merck cloud platform, which holds the corresponding private key, is able to decrypt it.



4. The Milli-Q® water system sends the session key to the platform along with its signed certificate to prove its identity. The Merck cloud platform verifies that it is a true, authorized Milli-Q® water system and not something else which is trying to usurp the identity of a Milli-Q® water system.





Now the Milli-Q® water system and the Merck cloud platform can communicate securely. All dialog is encrypted using the unique session key that they are the only ones to share.