SSH

CASE STUDY

Global IoT Device Provider Secures Maintenance Operations with PrivX® Privileged Access Management

Customer in a nutshell

- **Headquartered in Europe, the customer is a manufacturer of home appliances. The company's brand portfolio includes more than 10 well-known appliance brands.**
- **Turnover +10 B€**
- **+50K employees**
- **+35 factories world-wide**

Background

The customer is a global manufacturer of home applicances and is a well-established player in the global consumer market. They have headquarters in Europe but have branch offices all over the world with more than 50,000 employess in total.

As often is the case with geographically diverse companies, the customer has service and QA people in different locations around the globe. For upgrade and maintenance tasks, the staff needs access to IoT devices that offer home automation for the consumers. These target devices can be located anywhere anywhere in the world - just like the staff connecting to these devices.

The QA staff shared a "golden key" to access devices around the world, meaning that the same digital key opened access to all devices under the customer's purview. It's very convenient, since the key can be shared very quickly regardless of the location. Unfortunately, this approach is also very risky, since tracking the proper use of the key is challenging. Problems included verifying how you can:

> ***"We do not want to share our "golden keys" that grant access to our IoT devices, but we need to be able to connect to them from around the world!"***
> **- Customer QA admin**

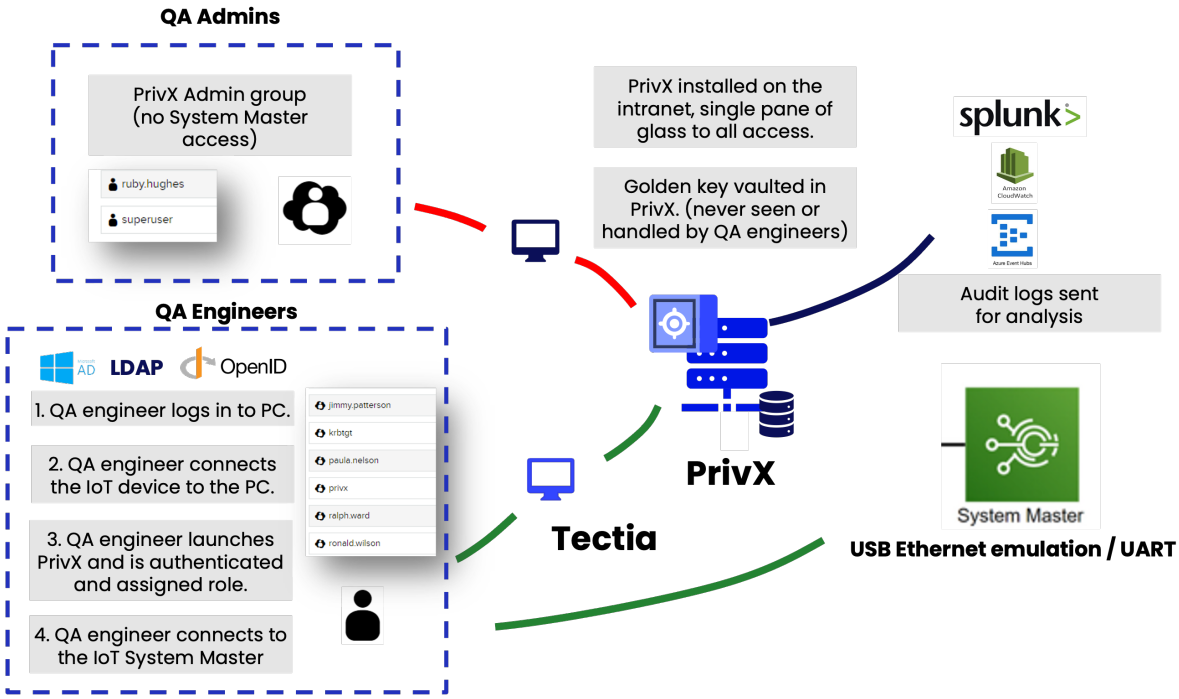
- identify the person using the key if it is shared between hundreds of members?
- ensure the key is not copied along the way
- make sure the key is not in the hands of an unauthorized user in the first place?

The customer was convinced that there had to be way to ramp up security while maintaining the flexibility and efficiency of using golden keys. To that end, they had tried to solve the problem in-house with various approaches – including using open source and professional tools but the challenge turned out to be bigger than anticipated. With the help of SSH/PrivX this challenged could be solved.

Secure, verifed access without shared credentials with PrivX.

With a few unsuccesful attempts to solve the challenge in-house, the customer started looking for outside help. After careful research and comparing vendors, they soon came to the conlusion that SSH's PrivX Privileged Access Management (PAM) solution would be ideal for their situation.

PrivX gave them the flexibility they needed. They started by deploying PrivX in the headquarters first and giving their team members around the globe secure remote access through a centralized control- without sharing the golden keys.



1. The QA engineer logs into a Windows PC and is authenticated by Active Directory.
2. The engineer connects the IoT device to his PC.
3. The QA engineer launches PrivX which identifies him automatically based on the AD authentication done earlier. PrivX also assigns the right privileges for the session based on the role.
4. The QA engineer initiates a connection to the IoT device to do maintenance tasks on the System Master with a secure remote software like PuTTy or SSH's Tectia Client.
    - The golden key is stored in a vault. The key is not exposed to the QA Engineer or anyone else nor can it be shared.
    - Only The QA Admin can upload the golden key to the vault or change it. These sessions are always audited, tracked or optionally recorded if needed. The QA admin cannot access the System Master.

The convenience of using shared credentials without their risk

After a quick Proof of Concept (PoC) phase, the customer was convinced that SSH was able to deliver the type of solution they were looking for. "Before committing to the solution, we wanted to test the suggested architecture", said the customer QA admin. "The POC was fast and easy to set up and we were able to see the results almost right way. Very happy to find a solution to our long existing problem", he continued.

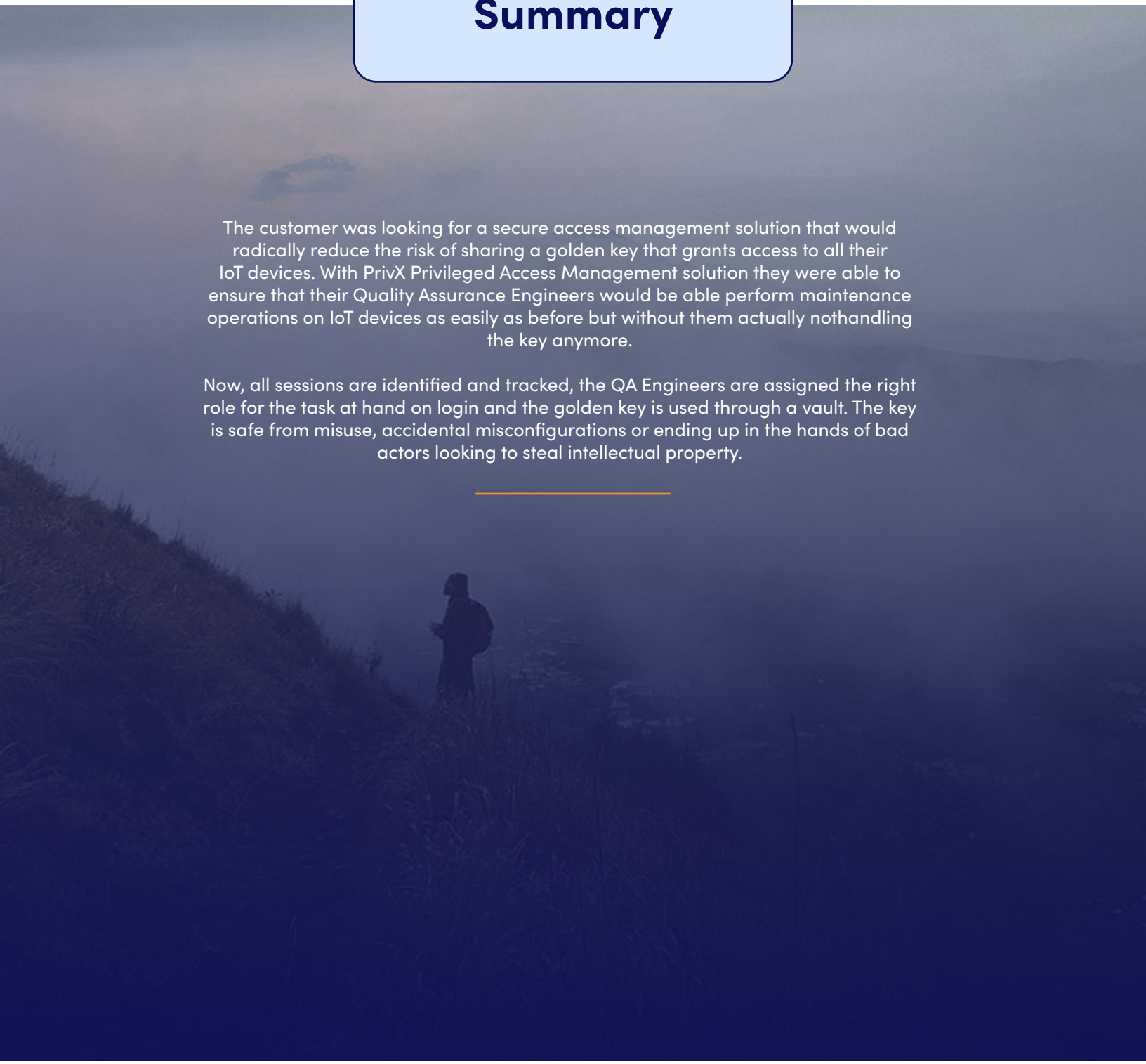
After the successful PoC, the customer continued to deploy the solution into production first in the headquarters, and then expanding its use to world-wide locations.

The customer QA engineer expressed his idea fo the main benefits of the solution. "Now there is no need to share the "golden keys" among many users anymore, since they can access the IoT device without ever handling or even seeing the credentials at any point of the process. This is a giant step forward in making our home appliances much safer than before".

On top of that, the customer was happy that there is no real need to change or rotate the "golden keys any longer, since only very few people have access to the keys. If there is a need to change the key, only a few QA admins can make the change, and their session are also tracked, audited or even recorded if needed.

> ***"Now there is no need to share the 'golden keys' among many users anymore, since they can access the IoT device without ever handling or even seeing the credentials at any point of the process. This is a giant step forward in making our home appliances much safer than before!"***
> **- Customer QA admin**

Summary



The customer was looking for a secure access management solution that would radically reduce the risk of sharing a golden key that grants access to all their IoT devices. With PrivX Privileged Access Management solution they were able to ensure that their Quality Assurance Engineers would be able perform maintenance operations on IoT devices as easily as before but without them actually nothandling the key anymore.

Now, all sessions are identified and tracked, the QA Engineers are assigned the right role for the task at hand on login and the golden key is used through a vault. The key is safe from misuse, accidental misconfigurations or ending up in the hands of bad actors looking to steal intellectual property.

Global headquarters
Helsinki

SSH Communications Security Corporation

Karvaamokuja 2 B 00380
Helsinki, Finland
+358 20 500 7000
info.fi@ssh.com

US headquarters
New York

SSH Communications Security, INC

434 W 33rd Street, Suite 842
New York, NY, 10001, USA
+1 781 247 2100
info.us@ssh.com

APAC headquarters
Hong Kong

SSH Communications Security LTD

35/F Central Plaza, 18 Harbour Road
Wan Chai Hong Kong
+852 2593 1182
info.hk@ssh.com