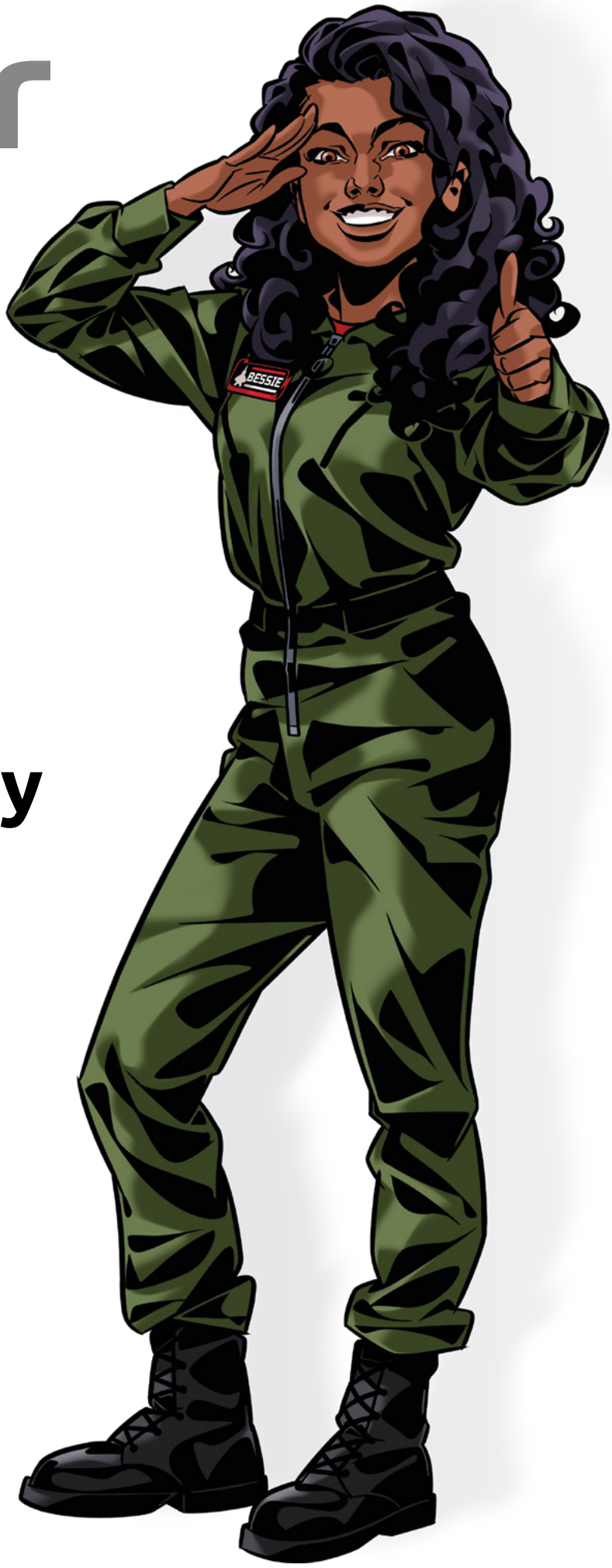
myQ roger



Data Security

Whitepaper
June 2022

MyQ, spol. s r.o., Harfa Office Park
Ceskomoravska 2420/15
Praha, 190 00, Czech Republic

Data Security Whitepaper

Introduction

The purpose of this document is to inform the customers of MyQ Roger about processes that involve establishing connection in the system and about security measures taken to protect consequent data transfer. The document also provides some additional resources with more information on security put in place by Microsoft for the Azure public cloud platform.

General information

Cloud security for MyQ Roger has been designed with all most relevant industry standards and best practises in mind.

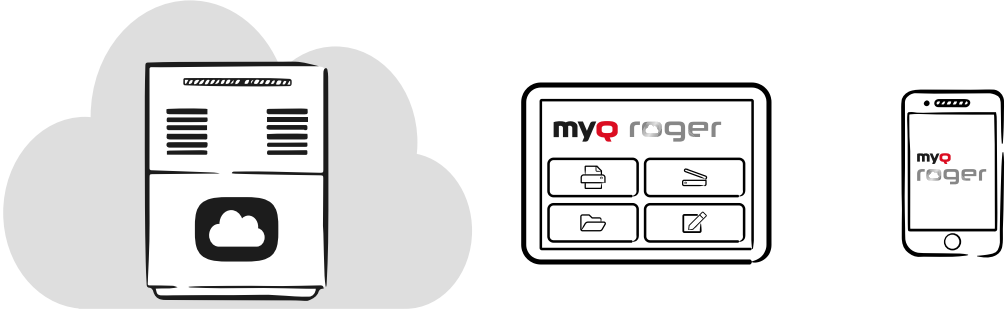
There are three instances of software that compose the MyQ Roger product:

a| the MyQ Roger server, running in Microsoft Azure (datacenters located in Ireland and USA)

b| the MyQ Roger embedded (EMB) client, running on the MFP

c| the MyQ Roger mobile application, running on the user's smartphone

All these parts of software establish connection with one another via port 443 (https://). The MyQ Roger server uses hostnames **api.roger.myq.cloud** and **app.roger.myq.cloud**.



Verification of the user with the server through the EMB client

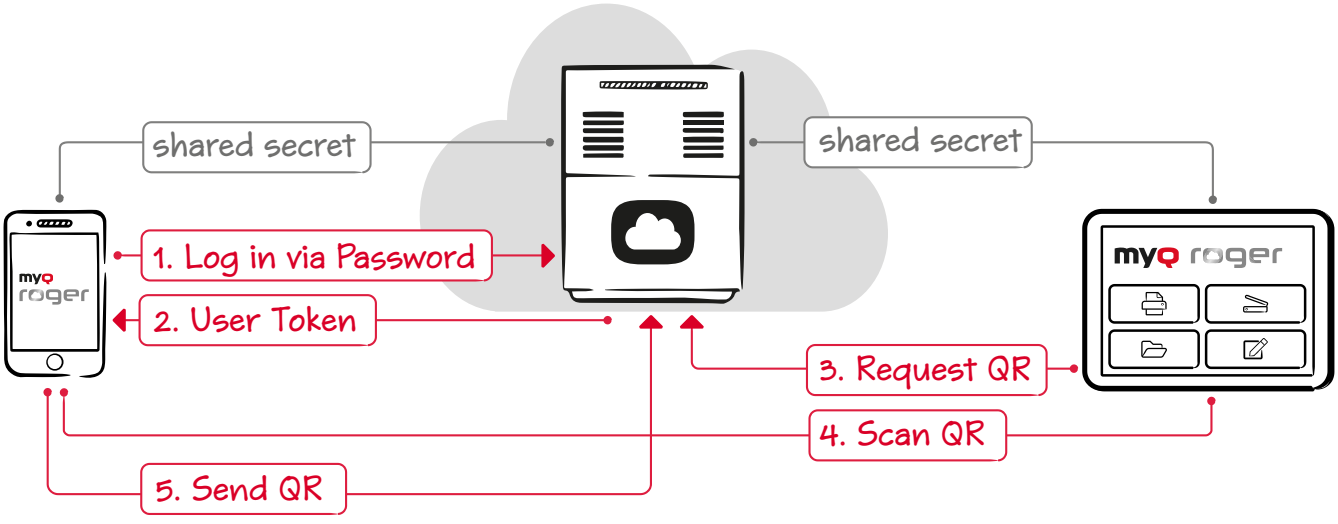
The EMB client is a MyQ application installed on the hardware of the multifunction printer, serving as a user interface. Communication between the cloud-based Roger server and the EMB client is established in order to verify and authenticate the given user with the MyQ Roger server (database) and to confirm the range of actions and rights available to that user within the MyQ Roger system.

The user intiates the user session by scanning a dynamic QR code off the touch panel of the MFP with the MyQ Roger mobile application. This prompts opening a secure connection between the EMB client to the MyQ Roger server. The security protocol used is **TLS 1.2,** and all relevant certificates are verified for each user session using SSL Labs, where MyQ Roger's overall rating is A+ (equivalent to internet banking security).

The authentication of the user (and EMB client) happens in two steps:

1. The EMB client verifies itself with the Roger server in compliance with the OAuth 2.0 Device Authorization Grant. The server is now ready to release the user's queued jobs on the MFP.

2. The EMB client performs a request for command in compliance with the Resource Owner Password Credentials Grant**.** The user can now submit new print jobs from their OneDrive or local storage and perform scanning actions at the MFP. After these two steps are performed, the EMB client is granted the right to call functions available to the authenticated user, on the user's behalf.



After these two steps are performed, the EMB client is granted the right to call functions available to the authenticated user, on the user's behalf.

Authentication Tokens

When the user is authorized with the Roger server, the server issues a unique **Access token** – a series of bytes that is impossible to breach. During the life of the token, which is around 20 minutes, users can access MyQ Roger functions without having to re-enter credentials each time they perform another action. Tokens also offer a second layer of security to the connection.

MyQ Roger also supports **Refresh tokens,** which have a longer life span than Access tokens (3 months). The MFP uses a refresh token with sliding expiration of 3 months. If the MFP is not used during this period, it is disconnected from the tenant and will not allow users to access MyQ Roger until it is reconnected again.

Access to data and data retention

When connecting the MyQ Roger application to the user's OneDrive for Business, the user grants MyQ Roger the right to browse and save to folders "Print" and "Scan" (they are created by MyQ Roger if they do not exist prior to connection). MyQ Roger will, however, request access to the user's entire OneDrive, just like other applications – this is due to a Microsoft limitation. Printed or scanned documents are not transferred through the MyQ Roger server, so the server does not modify or store their contents in any way. The server only verifies the user's available scanning profiles and printing functions. Document data exchange happens only between the user's connected cloud service (OneDrive for Business as of April 2021) and the MFP, which usually has encryption tools of its own in place, depending on the preference of the customer.

MyQ retains the following information about **print jobs:**

- User's email address
- User's full name or username
- User's PIN code/password (hashed)
- Printed document file name

MyQ retains the following information about **scan jobs:**

- time stamp of scan

All data retention is subject to governing laws and regulations (e.g. GDPR).

Microsoft Azure Public Cloud Resources on Data Security

Data contained in the user's OneDrive for Business fall under the protection of Microsoft, as the provider of the Azure cloud service. Microsoft's whitepaper on cloud security from 31/03/2021 can be found here: "Enabling Data Residency and Data Protection in Microsoft Azure Regions", and it covers the following topics (apart from others):

- How Microsoft protects customer data from unauthorized access, and how Microsoft handles and challenges government requests and other third-party orders
- The strict policies and practices that Microsoft follows for the retention and deletion of customer data
- How Microsoft compliance with privacy regulations and standards helps protect the privacy of customer data

More instructions on how to protect the customer's business environment in Microsoft Azure can be found in the Azure Security Center.