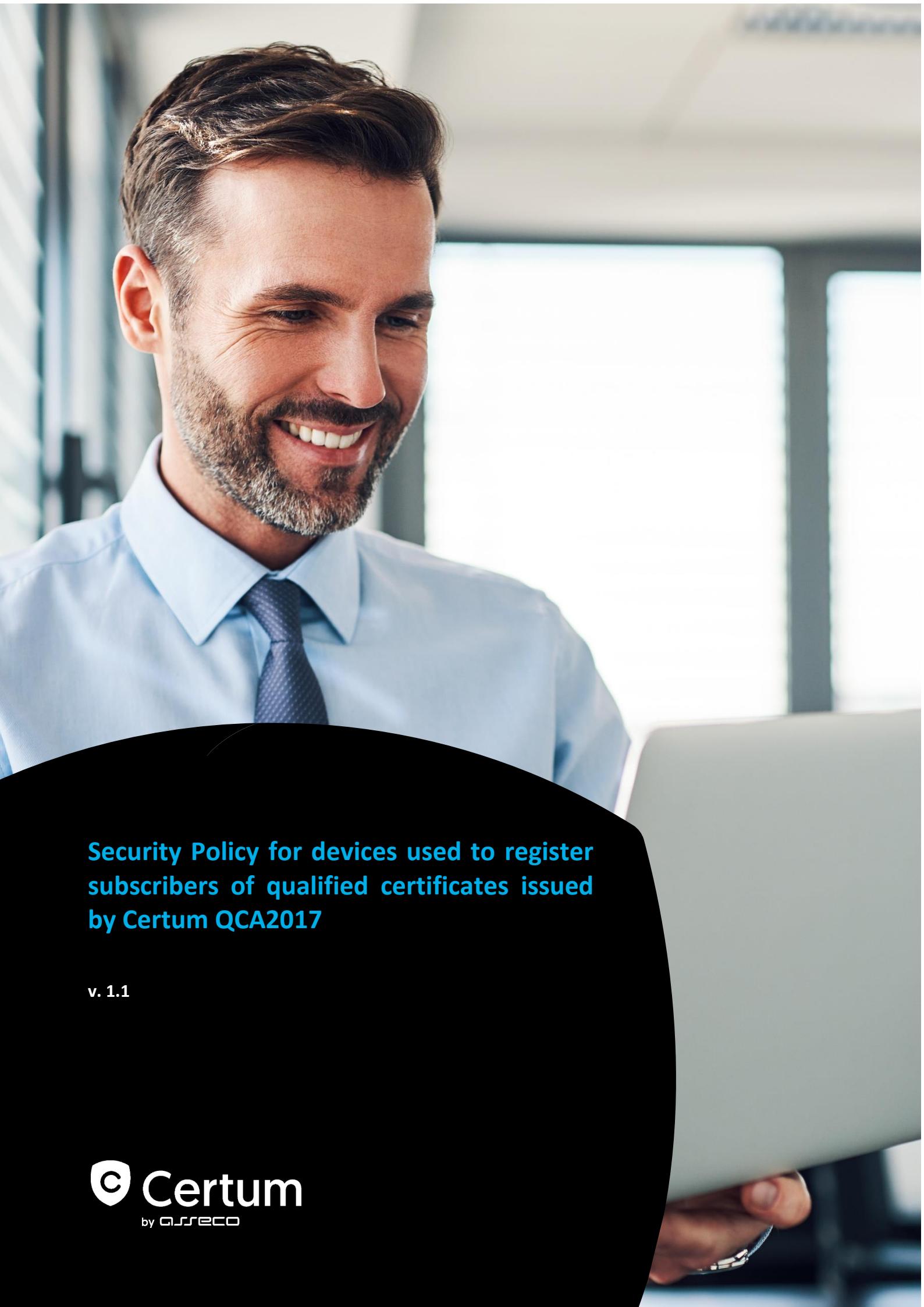

Security Policy for devices used to register subscribers of qualified certificates issued by Certum QCA2017

v. 1.1

Certum
by asseco

Trademark and Copyright notices

All the questions, concerning copyrights, should be addressed to Asseco Data Systems S.A., Jana z Kolna Street 11, 80-864 Gdańsk, Poland, e-mail: infolinia@certum.pl .

Table of contents

1	Registration and identification device	The device which is used to identify (also remotely) and register the certificate holder (Certum client).

Definitions

1	MDM	Mobile Devices Management. A system for managing mobile devices.
2	Paperless	A system produced by Certum for registering applications for the issuance of qualified certificates.

1. Administration of identification and registration devices

1. Registration and identification devices must be managed by Certum administrators:
    a) For mobile devices, through Certum's MDM system;
    b) For workstations, through the Asseco Data Systems domain controller.
2. With Certum's permission, device management by Certum Partner administrators is permitted:
    a) For mobile devices, through the partner's MDM system;
    b) For workstations, through the Partner's domain controller.
3. MDM systems and domain controllers must allow the rules of this security policy to be implemented without the device user being able to change the rules.

2. Protection of data recorded in the identification process

1. Data recorded in the identification process should only be processed on the device in a dedicated location (folder).
2. Data recorded during the identification process cannot be copied and transferred to external media connected directly to the device or online (to remote storage media) if these media are not under Certum's control.
3. The data recorded in the identification process must be deleted from the dedicated location on a regular basis in an automated manner, at least once every 24 hours.

3. Support for advanced biometric signature process

1. The registration and identification device must enable an advanced biometric signature recording at least three biometric characteristics. The signature is affixed to the certificate issuance statement. For this purpose, the device should record at least the following characteristics:
    a) stylus position,
    b) stylus speed dynamics,
    c) pressure of the stylus on the screen.

4. Support for hardware cryptographic key protection

1. The registration and identification device must be able to securely store the keys used to establish a TLS connection with client and server authentication (2-way TLS) in a local key store.
2. Keys stored in the local key store should be hardware protected, with no way to export them outside the device. Importing keys into the warehouse should be possible from within the MDM system or domain controller.
3. The browser the user uses to connect to the Paperless system should support establishing a TLS session with client authentication using keys stored in the local key store.

5. Managing system updates (including security patches)

1. Identification and registration devices should have all system updates, including security patches, made available by the manufacturer installed.
2. Installed security updates should eliminate critical and high level vulnerabilities.
3. Installed security updates should be no older than 6 months.
4. Where security updates are not issued by the device supplier, the device may be used to communicate with Certum's systems as long as alternative security features acceptable to Certum are implemented to mitigate the likelihood of attacks on the integrity or non-repudiation of the identification or registration process.
5. The security measures set forth in item 4 will be reviewed periodically as part of the risk analysis. If the level of risk increases and is no longer acceptable to Certum, Certum reserves the right to withdraw the devices from use immediately.

6. Acceptance of identification and registration devices by Certum

1. Identification and registration devices are subject to recording and approval by Certum administrators.
2. Prior to being placed in service, Certum administrators should be notified of each new device model, together with a statement that it meets all the requirements of this policy.
3. The device subject to notification, after acceptance by Certum administrators, can be used in identification and registration processes only after the key used to establish two-way TLS authentication with the qualified certificate application signing module is installed on it.
4. The key installation is carried out by Certum administrators or Partner administrators only on approved devices.

7. Removal of identification and registration devices by Certum

1. If this security policy is violated, Certum administrators may revoke without warning the TLS certificate used to establish a secure connection to the qualified certificate application signing module.