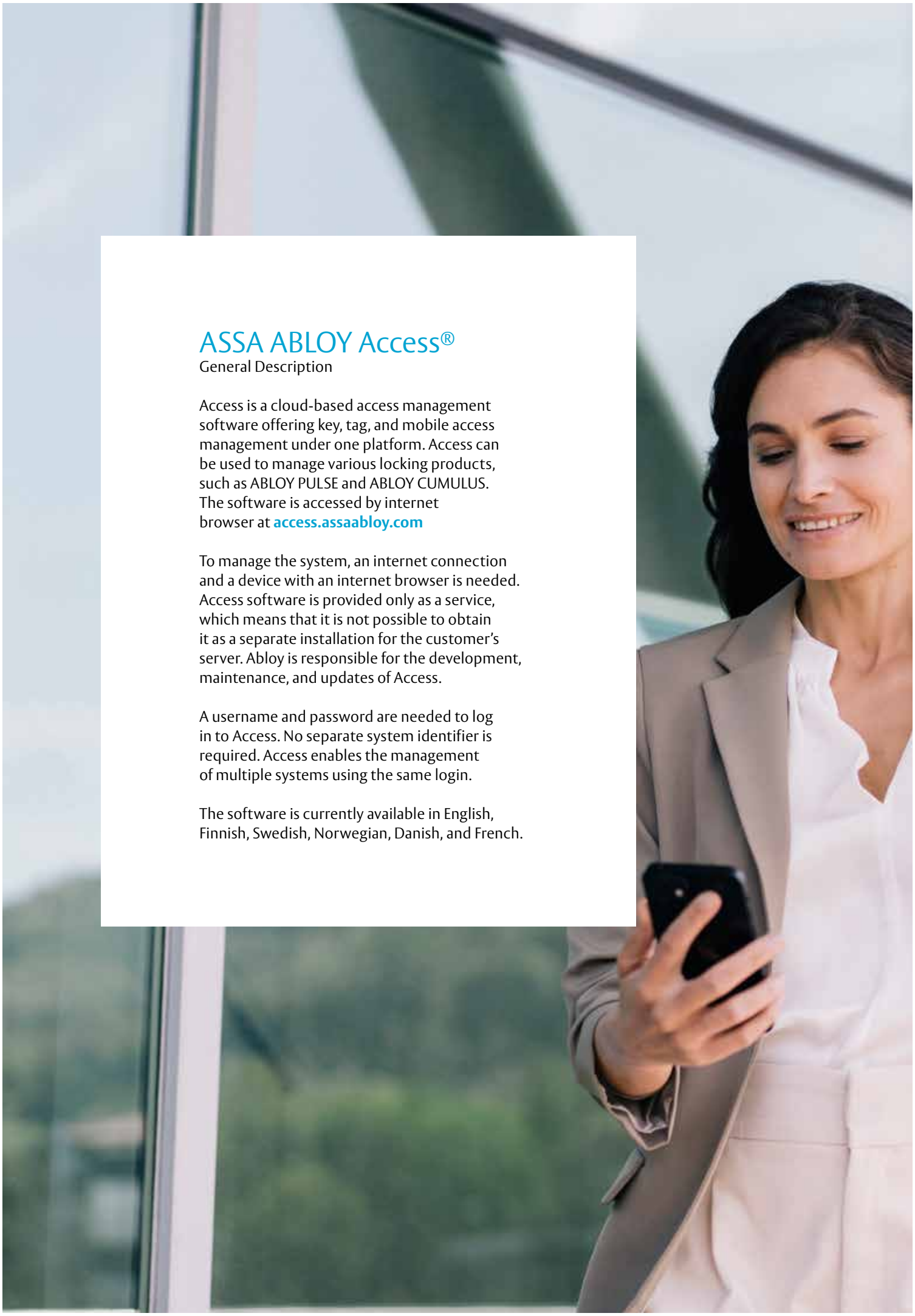
ASSA ABLOY Access®
Technical Brochure

ASSA ABLOY
Opening Solutions

Experience a safer
and more open world

Contents



ASSA ABLOY Access®

General Description

Access is a cloud-based access management software offering key, tag, and mobile access management under one platform. Access can be used to manage various locking products, such as ABLOY PULSE and ABLOY CUMULUS. The software is accessed by internet browser at **access.assaabloy.com**

To manage the system, an internet connection and a device with an internet browser is needed. Access software is provided only as a service, which means that it is not possible to obtain it as a separate installation for the customer's server. Abloy is responsible for the development, maintenance, and updates of Access.

A username and password are needed to log in to Access. No separate system identifier is required. Access enables the management of multiple systems using the same login.

The software is currently available in English, Finnish, Swedish, Norwegian, Danish, and French.

ASSA ABLOY Access
Software as a Service (SaaS) content

ASSA ABLOY Access SaaS is maintained on an Amazon Web Services (AWS) platform. The service uses an AWS data centre located in Ireland, where the Access software operates in two different availability zones.

Amazon Web Services (AWS) carries the ISO27001, ISO27017, ISO27018, and SOC1-SOC3 certifications. For more information, see the Compliance section on the Amazon Cloud website at **aws.amazon.com/compliance**

The infrastructure is based on the principle of high AWS availability, where each instance has an active and a passive server. This allows for quick recovery from problems and maintenance in transfer mode between servers.

ASSA ABLOY System Manager

System Manager is a service portal through which ABLOY- authorised resellers manage ASSA ABLOY Access customers and their systems. The portal allows the resellers to set up the main users of the applicable system and user credentials for installers to log in to the ABLOY PULSE mobile application. Administrators are also able to set up other administrators, installers, customers and systems. The system setup process defines basic information, such as the system name, customer name (system owner), and selects the IDs of the installers who can view the system information in the mobile application.

Features

1. Accessibility and usability
- Enables system management independently of time and place with a computer
- Automatic software updates, security updates and backups
- Basic use of the software does not require software installations (except for the desktop reader)

2. Login
- A username and password are needed for management of the system (without a separate physical programming identifier)
- Multi-system management is possible

3. Design of the site, users and products
- Addition and editing of buildings, floors and floor plans
- Creation and editing of products and user information
- Handover and return of keys with option to print handout document of keys
- Management of locks and readers using the floor plans

4. Mass data importing
- Importing of products, keys, persons and access rights using Excel templates

5. Access rights
- Setting, change and deletion of access rights
- Management of validity periods for keys
- Management of lost keys
- Management of access rights groups and access rights profiles
- Management of PIN codes
- Locking chart export in Excel format

6. Audit trails
- Collection and display of audit trails for keys, locks and updaters (optional)
- The events of the audit trails are collected automatically via the updater

7. System administrator roles
- Specify the functions of the locking system that the administrator is authorised to perform
- The functions are displayed in the software depending on the role assigned to the administrator

8. User-friendly user interface
- Dashboard with locking system statistics
- Logical menu structure
- Responsive web design

9. General system settings
- Revalidation period setting for keys
- Retention period setting for audit trails and event logs
- Handout document templates

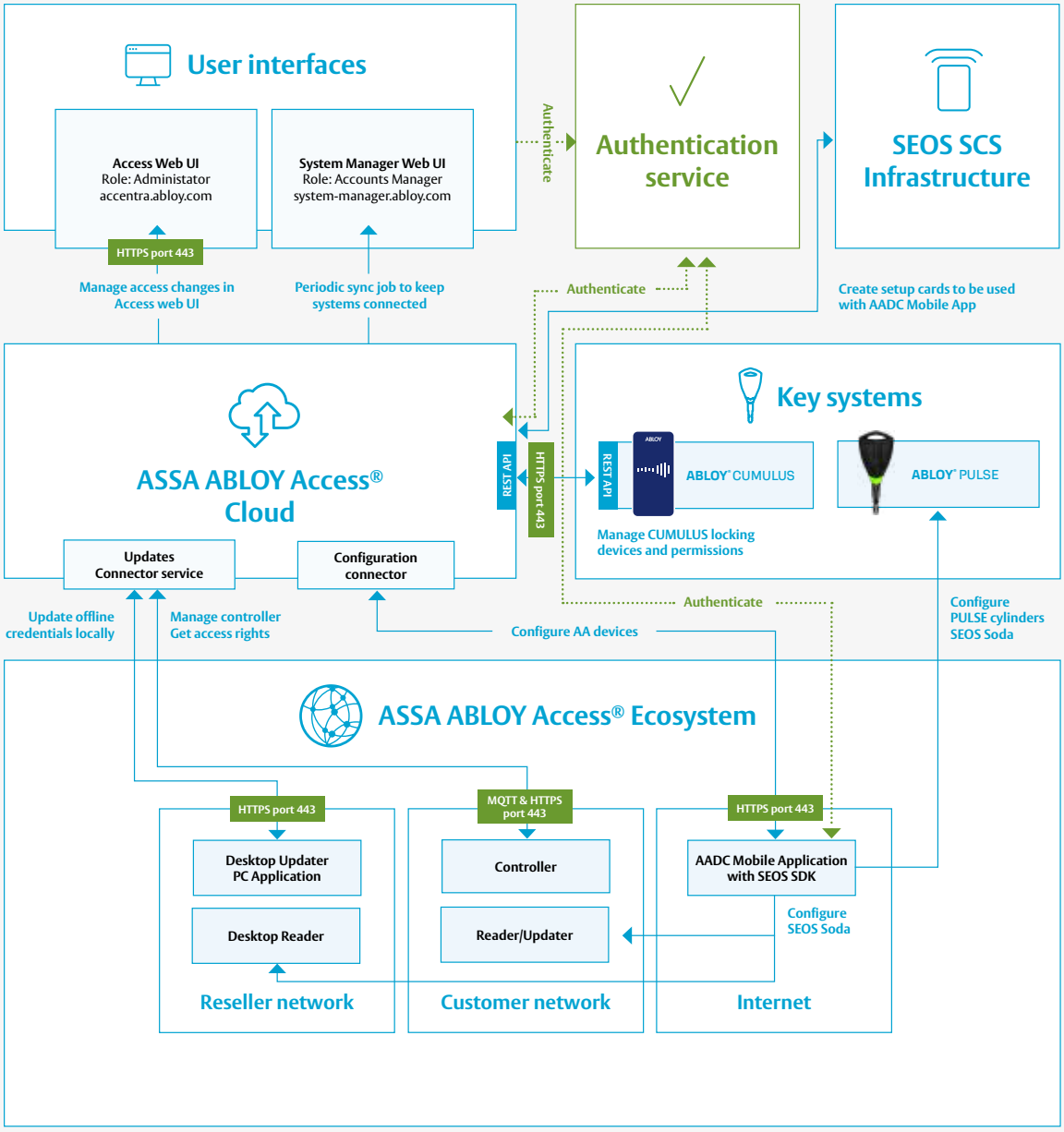
ASSA ABLOY Access Architecture and Network Diagram

Access Cloud is built using microservices in Amazon Web Services and is hosted in AWS Ireland. AWS infrastructure diagram is shown later in the document for reference. All the connections are encrypted and running in either HTTPS or MQTTS.

Desktop Updater PC application and Door Controller are hosted in reseller and customer networks respectively. Door Controller communicates with Access cloud using encrypted MQTT protocol on port 443 and uses HTTPS as a fallback method. Access Cloud has REST API which enables 3rd party integrations to extend the functionalities. Keyless locking system, ABLOY Cumulus, for example, utilises this REST API.

The diagram below describes the Access ecosystem and network with the essential system components and their relations.

ASSA ABLOY Access®



Desktop Updater

Necessary network URL's
the Desktop Updater shall have access to:

- access.assaabloy.com
- europe1.system-manager.assaabloy.com
- accentra.abloy.com
- accentra.assaabloy.com

All running in port 443 HTTPS TCP

Door Controller

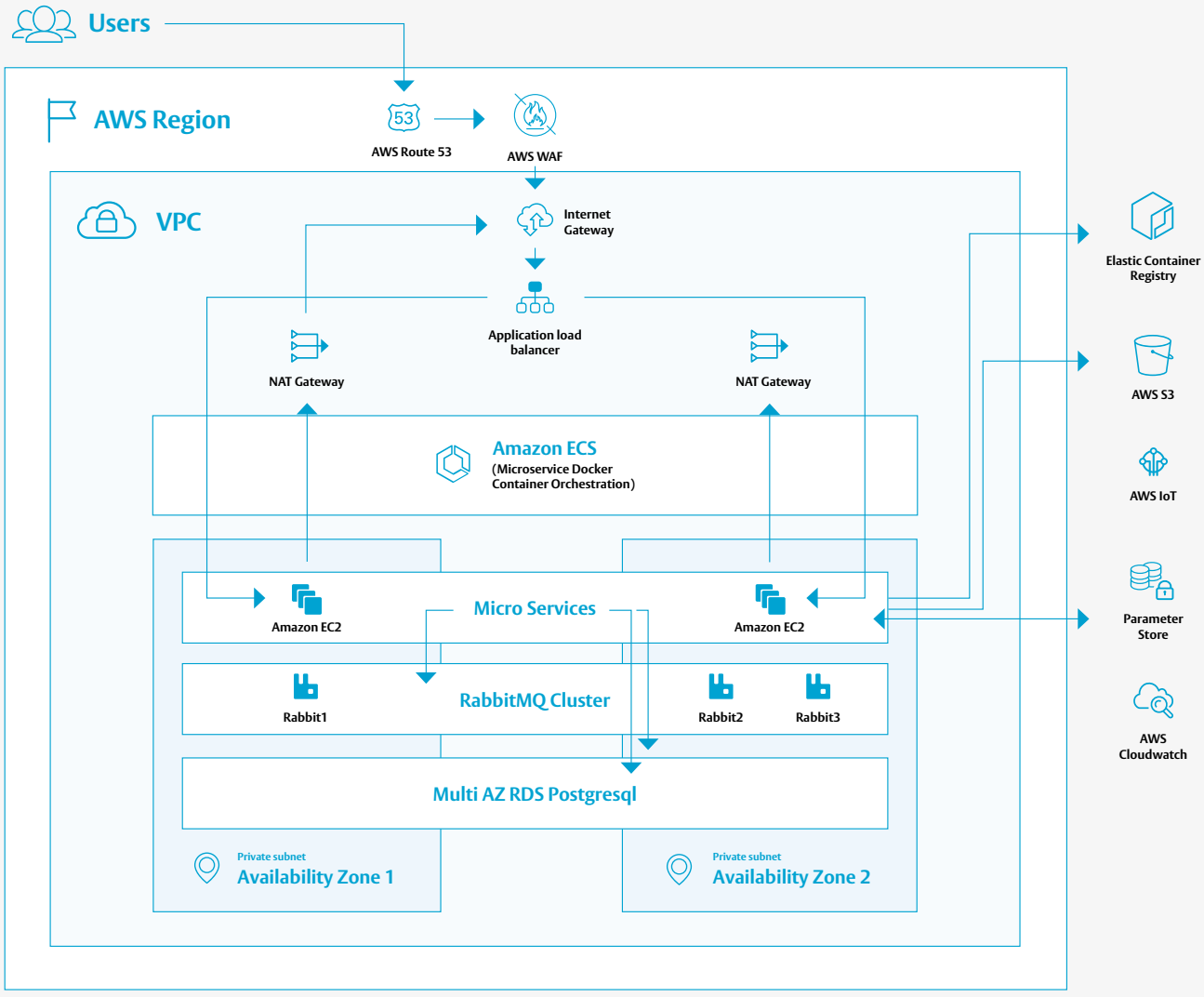
Door Controller can be setup with static IP's or used with DHCP server. Door Controller shall have the following protocols and ports and URL's accessible through firewall.

- MQTT and HTTPS port 443
- NTP port 123
- DNS port 53
- Access to following URL's accessible:
  - access.assaabloy.com/*
  - accentra.abloy.com/*
  - accentra.assaabloy.com/*
  - rocketfw.s3-eu-west-1.amazonaws.com/* (used for firmware updates)
  - a2118gv0vua4gp-ats.iot.eu-west-1.amazonaws.com (MQTT broker address)

* refers to all sub URL's under the same domain

AWS Infrastructure Diagram

- Region – Ireland
- WAF – Web Application Firewall
- Running in AWS EC2 instances
- Application Load Balancer
- Database in RDS PostgreSQL
- Queueing is using RabbitMQ



Data Security and GDPR

Security of data communications

ASSA ABLOY Access infrastructure is built on a public cloud platform (Amazon Web Services). Access has a separate private cloud and advanced firewall rules and access control that restricts access from the outside and inside of the network to trusted sources only. Access to servers is limited to functionality and support team members and to read-only access. All the licensees have undergone a background check based on ASSA ABLOY's security policy, and access rights are audited twice a year.

Communication between all the services and devices is protected by HTTPS and by the use of the TLS mechanism to validate server certificates. In the PULSE system, data communication and the data packet it contains are separately encrypted, making the system extremely secure.

The following table describes the mechanism for securing communications between ASSA ABLOY Access and physical devices.

Service	External device / application	Protocol and security mechanism
Access	ABLOY PULSE mobile application	The application acts as an HTTPS client. The application ensures communication with the correct service with a certificate and uses an access token (OAuth) to authenticate to the service.
Access	Internet browser	The application acts as an HTTPS client. The application ensures communication with the correct service with a certificate and uses an access token (OAuth) to authenticate to the service. Communication is protected using the HTTPS protocol. The browser is responsible for validating the server certificate provided by Access.
Access	Updater	MQTT with TLS and HTTPS data communication protection is used. The firmware ensures communication with the correct service using a certificate. Updating of sensitive data in the reader memory is protected by SeoS encryption.
Access	Desktop reader / PC software	HTTPS data communication protection is used. The application ensures communication with the correct service using a certificate.
CUMULUS	CUMULUS Application and locking devices	Each operating device is registered to the CUMULUS ecosystem and is given a certificate which is used to securely communicate to CUMULUS backend and with the locking device.
CUMULUS	Integration	All integration between Access and CUMULUS is secured and goes through API's.

Data storage

The databases used in Access are backed up every six hours and stored in a separate service in AWS. Backups are kept for 30 days.

Access collects application-level logs about system activity. Sensitive information such as passwords is not stored in the log data. Log retention varies between services, but the longest retention period is 30 days. Similarly, logs related to infrastructure are managed and audited by the service development team. Only authorised personnel have access to log storage, and views are also recorded in the logs. Infrastructure-related logs are retained for two weeks.

Data security

Abloy Oy is part of ASSA ABLOY Group. In accordance with ASSA ABLOY's rules, we are committed in our business operations to acting in accordance with best ethical practices and to complying with applicable legislation. Abloy is committed to continuously reviewing its processes and guidelines.

In the ASSA ABLOY Access system, Abloy is always the data processor. Abloy processes personal data only on behalf of the customer. Abloy never processes personal data for purposes other than those specified by the customer. The end customer is the data controller that has stored the data in the system.

In the development of the Access system, we adhere to the principle of privacy by design and carry out data security impact assessments.

ASSA ABLOY Group believes that the disclosure of vulnerabilities is essential for improving the quality of our products and services, the safety of our customers that rely on them, and awareness as to their choices relative to preserving their specific interests. ASSA ABLOY values insight from the security research community and welcomes disclosure and collaboration with this community. More information and the Policy can be read from Assa Abloy Product Security pages. Product security | ASSA ABLOY

We are committed to following the best practices in Secure Software Development Life Cycle (SSDLC) to ensure everything is developed with security in mind. SSDLC is used to identify and mitigate potential security vulnerabilities and threats during the development so the final product will be secure by default.

ABLOY® PULSE

General Description

ABLOY PULSE is an advanced locking and access management system, that can be considered an ecosystem in which keys and locks communicate with each other. The ecosystem covers customer locking requirements including access management and locking solutions. Cylinders, padlocks and furniture locks, RFID readers and keys can be connected to the system. The system is managed with ASSA ABLOY Access software.

ABLOY® CUMULUS

General Description

ABLOY CUMULUS is a keyless locking system enabling versatile access using the mobile device instead of physical key or token.The mobile phone carries the permission to open a given device rather than defining permission in the lock itself, and takes care of getting audit trails from the locks to the cloud.

Locking devices can be operated using mobile phone even without online connectivity when the access keys are loaded onto the mobile during online usage before accessing the offline lock.

CUMULUS portfolio includes mobile keys, padlocks, key deposits, controllers, swing handles and firmware. Locking devices integrate to digital tools offering reliable and fluent operations in conjunction with the Access Management System. CUMULUS integrates to ASSA ABLOY Access and access permissions are managed via Access Web UI.

Online updater

The updater is the central element of the PULSE system and the HID Key Fob funtionality. The updater consists of a controller and an RFID reader that is connected to it. The controller is connected via the internet connection to Access, making the system remotely controllable. The updater makes it possible to change key access rights and update data to the keys. Users' keys also transfer data from the locks to the software without the need for an administrator to visit the property.

The updater can also be used to control a door, lift or gate that is connected to the controller. In principle, it can be used to control any relay-controlled device. The controller's memory stores the system's access rights in encrypted form, making it possible to use the door even if the connection to the cloud service is not working.

The system can consist of one or more updaters. The controller can be connected to one reader and can be used to control one door. The controller is compatible with the PULSE Signo 20 and 20K readers. Even if the internet connection is cut off, up to 1,000 previous access events and 20,000 key permissions can be stored in the memory.

Technical specifications of the controller

Input voltage	12 to 24 Vdc +/- 10%
Ethernet Communication	10BaseT/100Base-TX
Reader Power	12 Vdc +/- 10% regulated, 500 mA maximum each reader
Operating Temperature	32 to 158 °F (0 to 70 °C)
Dimension	6.46" x 5.51" x 1.02" (164 mm x 140 mm x 26 mm)
Weight	352 g
Reader support	max. 2 readers

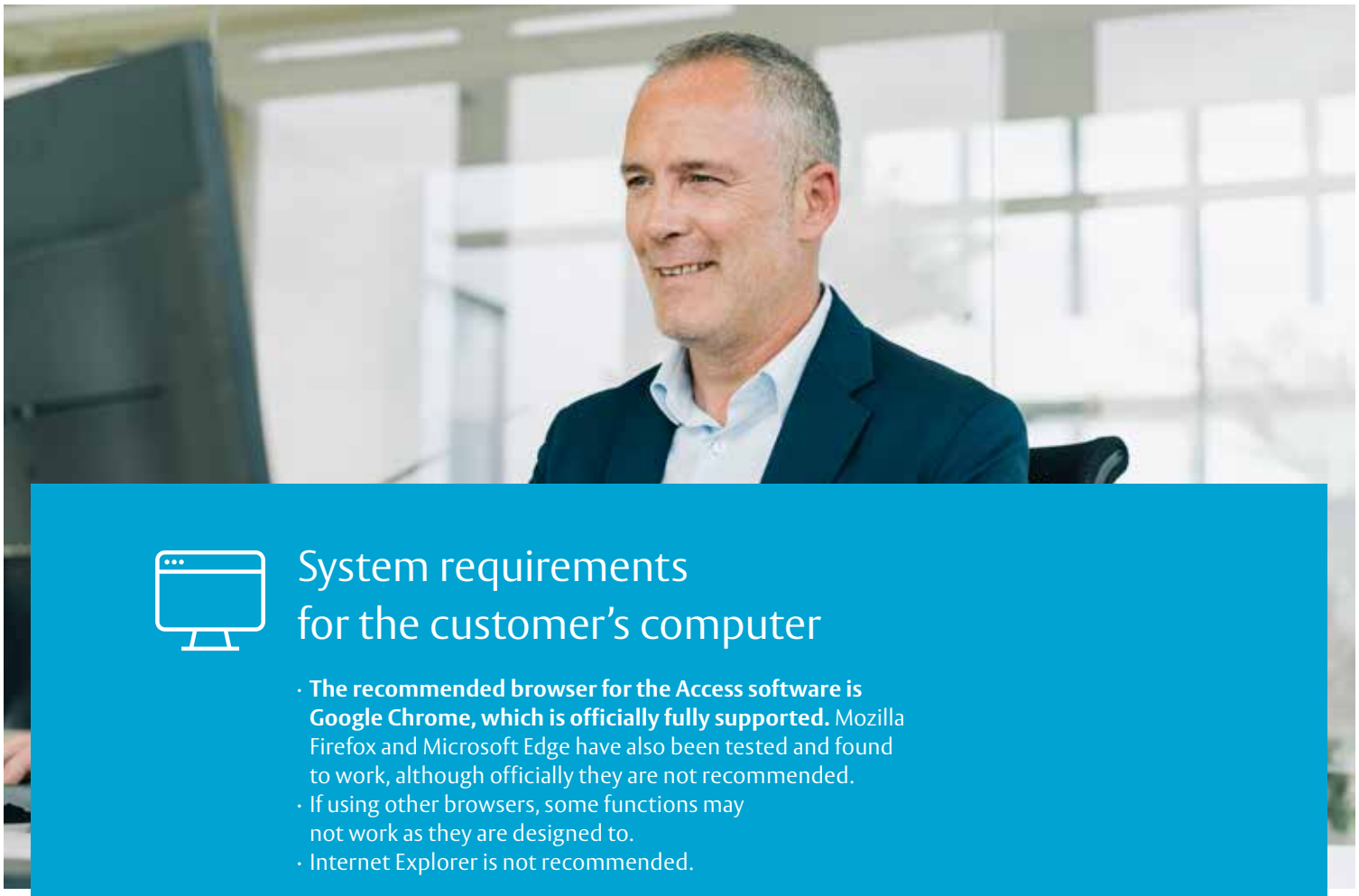
Technical specifications of the reader

	Signo 20	Signo 20K
Color	Black or white with silver trim baseplate	Black with silver trim baseplate
Operating Voltage	12V DC	12 DC
Keypad	No	Yes (2x6 layout)
Dimensions (width x length x depth)	1.77 in x 4.78 in x 0.77 in (45 mm x 121.5 mm x 19.5 mm	1.78 in x 4.79 in x 0.85 in (45 mm x 121.5 mm x 21.5 mm)
Environmental Rating	UL294 Outdoor and Indoor rated, IP65	UL294 Outdoor and Indoor rated, IP65
Transmit Frequency	125 kHz, 13.56 MHz, and 2.4 GHz	125 kHz, 13.56 MHz, and 2.4 GHz
Operating Temperature & Humidity	-31° F to +150° F (-35° C to +66° C) 0% to 95% non-condensing	-31° F to +150° F (-35° C to +66° C) 0% to 95% non-condensing

Key fobs

ASSA ABLOY Access will enable digital access management and tags in conjunction with PULSE or mechanical keys. Key tags enable flexible access possibilities where PULSE keys are not required but access to e.g. common areas, gyms or garages is needed. Key fobs can be used to provide access for 3rd party users requiring access to common areas but no access to the more private premises inside the building.

More information can be found from product specific technical brochures.



System requirements for the customer's computer

- **The recommended browser for the Access software is Google Chrome, which is officially fully supported.** Mozilla Firefox and Microsoft Edge have also been tested and found to work, although officially they are not recommended.
- If using other browsers, some functions may not work as they are designed to.
- Internet Explorer is not recommended.

Customer internet connection requirements

The Access controller communicates with Access via internet connection. The most common internet interfaces available from operators are suitable as the internet connection. The recommended interface speed is at least 10Mbit/s. If using a mobile broadband connection, a subscription with unlimited data transmission is recommended.

Depending on the network infrastructure, the controller is connected to the router or switch using a network cable with an RJ45 connector. The controller automatically retrieves the IP address and other necessary network settings from the DHCP service on the network. If no DHCP service is found on the network, the network can be manually configured.

The Access controller maintains contact with Access, during which time the changes that are made can be updated to the key with a delay of about 10 seconds (depending on the speed of the internet connection and the environmental load on the server). The controller can decide independently to open the door, so, disconnection of the network does not prevent the door from being used if the key is programmed into the system and if the key has access rights to the door controlled by the controller. However, when the network connection is disconnected, key data cannot be updated to Access, nor can the key be updated with changed access rights.

In principle, separate firewall rules are not required by the controller's data communications since the direction of data transmission is from the internal network to the internet. In firewalls, return packets are usually allowed automatically. The firewall and necessary network settings can be verified by the network administrator. The controller must have access to the public internet via the TCP 443 port.

The ASSA ABLOY Group is the global leader in access solutions. Every day, we help billions of people experience a more open world.

ASSA ABLOY Opening Solutions leads the development within door openings and products for access solutions in homes, businesses and institutions. Our offering includes doors, door and window hardware, locks, access control and service.

ASSA ABLOY
Opening Solutions

ABLOY UK
Portobello Works
School Street
WV133PW
England

Tel. +44 (0) 1902 364 500
www.abloy.co.uk