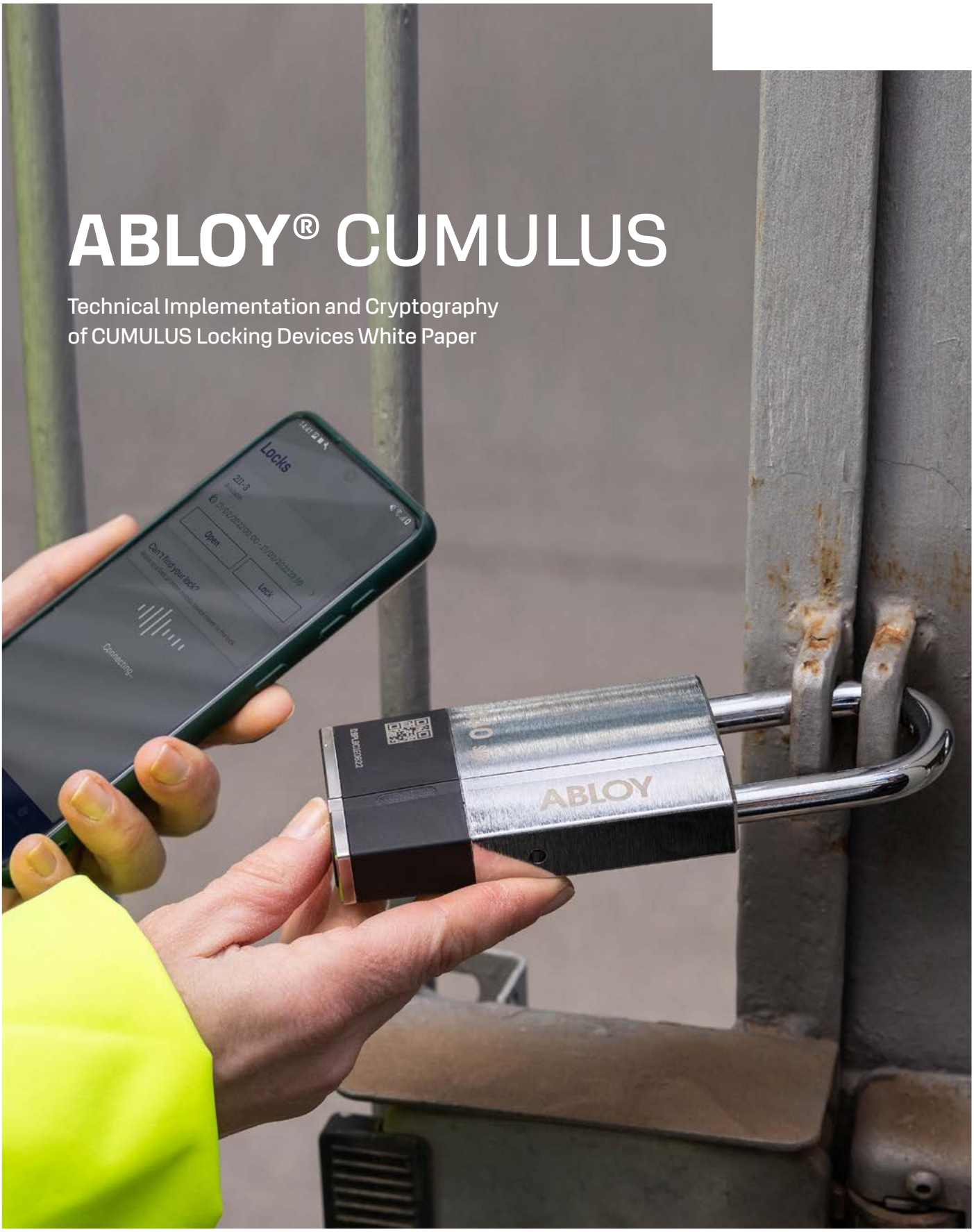
ABLOY® CUMULUS

Technical Implementation and Cryptography
of CUMULUS Locking Devices White Paper

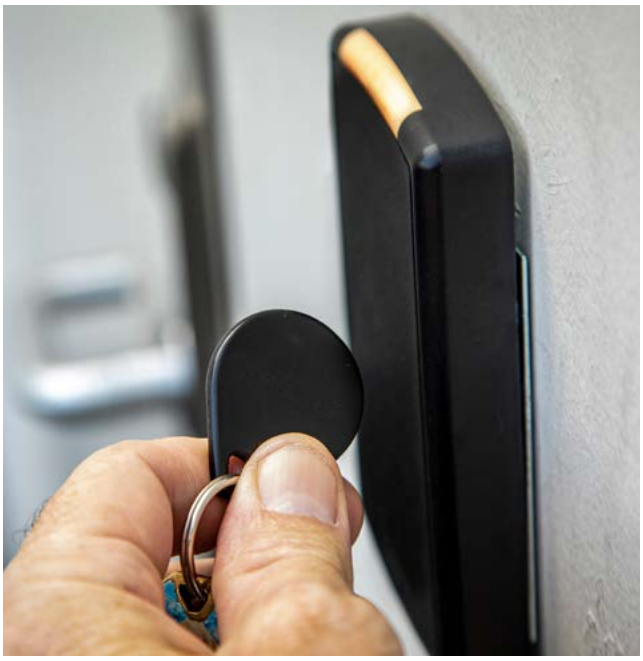


ABLOY

CONTENTS

Introduction

Exciting digital innovations have transformed locking solutions in recent years. Digital locks have been in trusted use for decades, for example, key fobs and cards are digital replacements for unique physical keys – but while they look different from keys, they feel very similar in use. That is, you need to give something to a user to carry around to access different sites they plan to visit.



What exactly has changed then? The current evolution is that users are given more fluid access as needed across organisations while using no extra physical devices. In practice this means that instead of handing out keys, people can use their personal devices like smartphones to open locks. In our unique solution the user brings the access rights straight to a lock. In this whitepaper we explain in further detail how to deliver secure access to a user, and how to communicate to a lock which user should have access and when.

CUMULUS Architecture

CUMULUS architecture was designed to meet future demands of access management. The premise was that we cannot presume the lock is always online, and we should also assume a user needs access to various locks at different times. We also wanted a stand-alone solution, where no physical key or fob must be provisioned, and locks gain access information independently, without having to program the locks in any way.

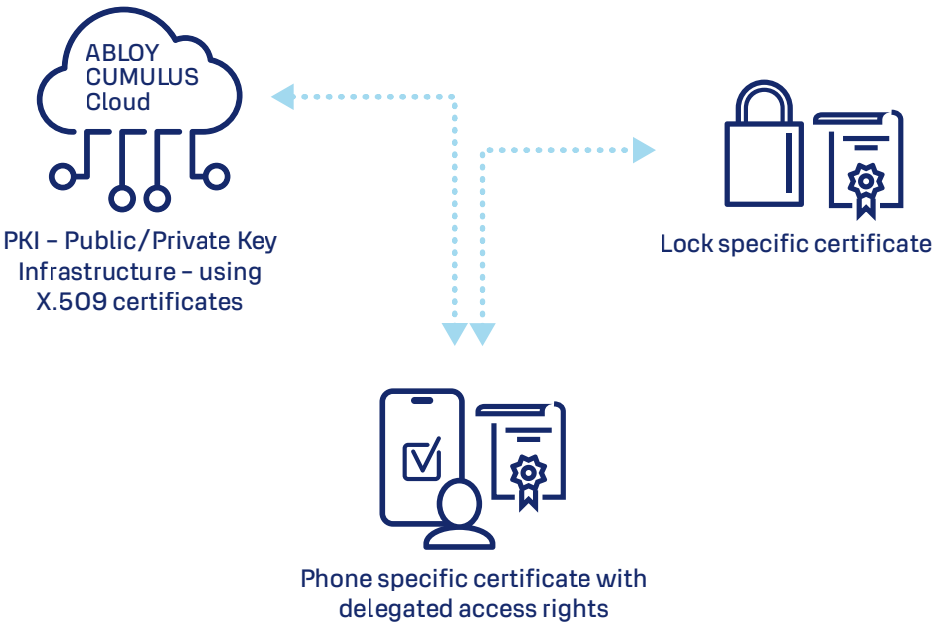
In this solution, a lock owner first creates a single-use invite. The invite is sent via SMS or email to a user's device and requires action within a customisable time period, or the link will expire. The user will get a certificate, that represents their identity in the CUMULUS ecosystem. Once an invite link is used, it cannot be reused.

In practice, when a new user needs access, we wanted to be able to provision the user with access payload even while being physically unavailable to connect to a lock. We explain access payload further in the next paragraph, but for this to work, when a user needs to use a lock, the lock should trust what is presented by the user. To do this, we created a Public Key Infrastructure (PKI) scheme.

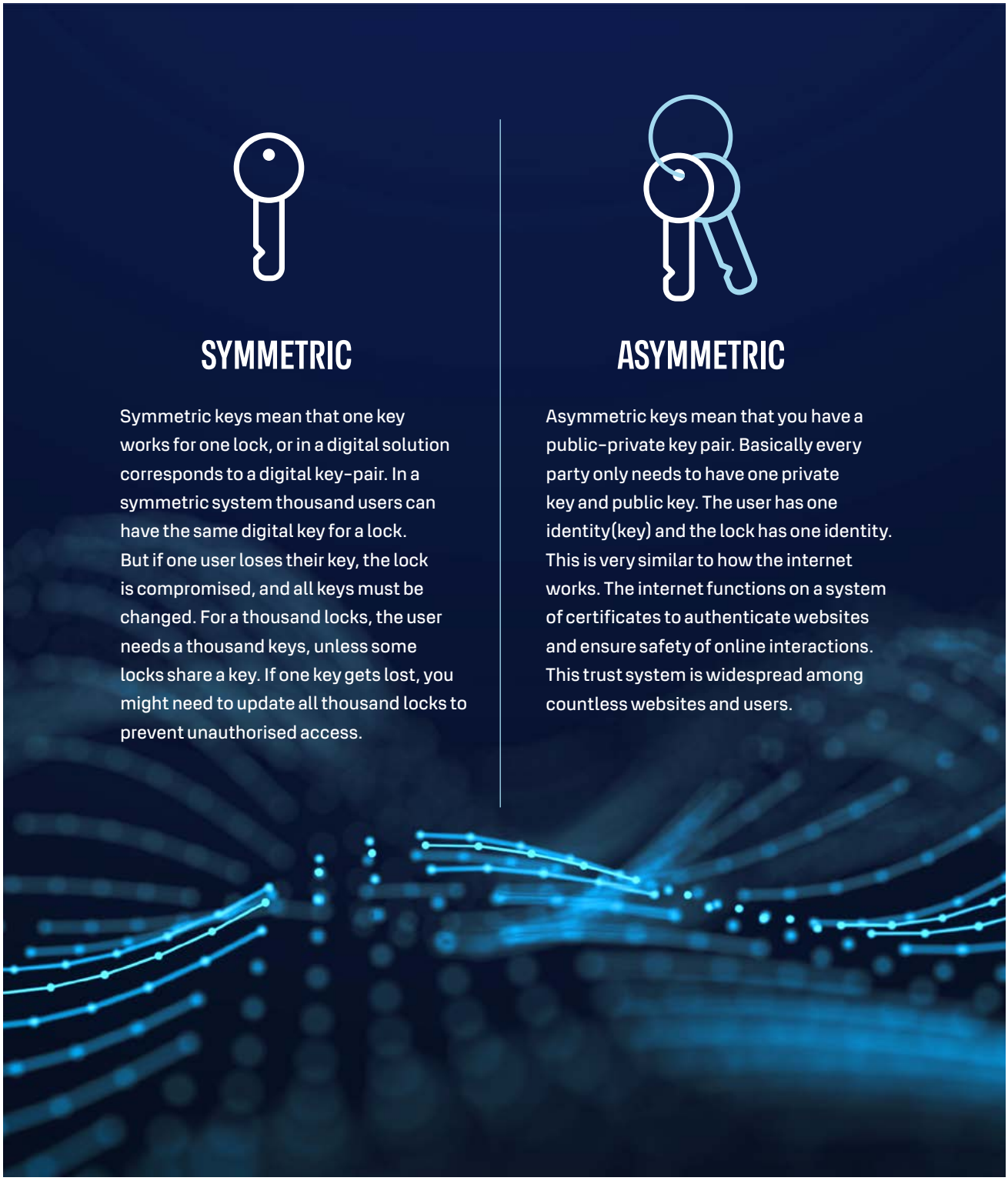
Utilising PKI means that the lock has a unique identity and the provisioned user's device, like their smartphone, has a unique identity. This way we can cryptographically give a user specific access to a specific lock for a specific time. We call this the access payload. The access payload can be given to the user as it is encrypted in a way that only a single lock in the world can decrypt and read the message.

In our solution, you always need to provide two things to the lock: the access payload, and a user's device identity. The phone user cannot read or modify the access payload, and the access payload has the user's identity so that the lock can identify the user's device, meaning it is not possible for someone else to use the same payload. Most smart devices also have default features that protect them from unknown users, for example smartphones have face recognition to securely unlock a personal device.

CUMULUS architecture works on a simple basis that allows us to provision access payloads to users even when they are not physically near a lock.



Symmetric vs. Asymmetric



SYMMETRIC

Symmetric keys mean that one key works for one lock, or in a digital solution corresponds to a digital key-pair. In a symmetric system thousand users can have the same digital key for a lock. But if one user loses their key, the lock is compromised, and all keys must be changed. For a thousand locks, the user needs a thousand keys, unless some locks share a key. If one key gets lost, you might need to update all thousand locks to prevent unauthorised access.

ASYMMETRIC

Asymmetric keys mean that you have a public-private key pair. Basically every party only needs to have one private key and public key. The user has one identity(key) and the lock has one identity. This is very similar to how the internet works. The internet functions on a system of certificates to authenticate websites and ensure safety of online interactions. This trust system is widespread among countless websites and users.

PKI Infrastructure and identities

As stated, we are using Public Key Infrastructure (PKI), further meaning we use Public Key Cryptography and certificates to be able to identify different parties. By using Digital Certificates, all parties can verify each other's identities and establish secure communication channels between them.

This is a well-known technology and an industry standard. It is also the recommended way for Internet of Things devices to authenticate themselves by using standardised certificates such as the X.509 standard.

We are using services such as Hydrant ID, an industry leading certificate authority service, and SEOS trusted service manager (TSM), a secure key-delivery mechanism for mobile phones and part of the Seos ecosystem.

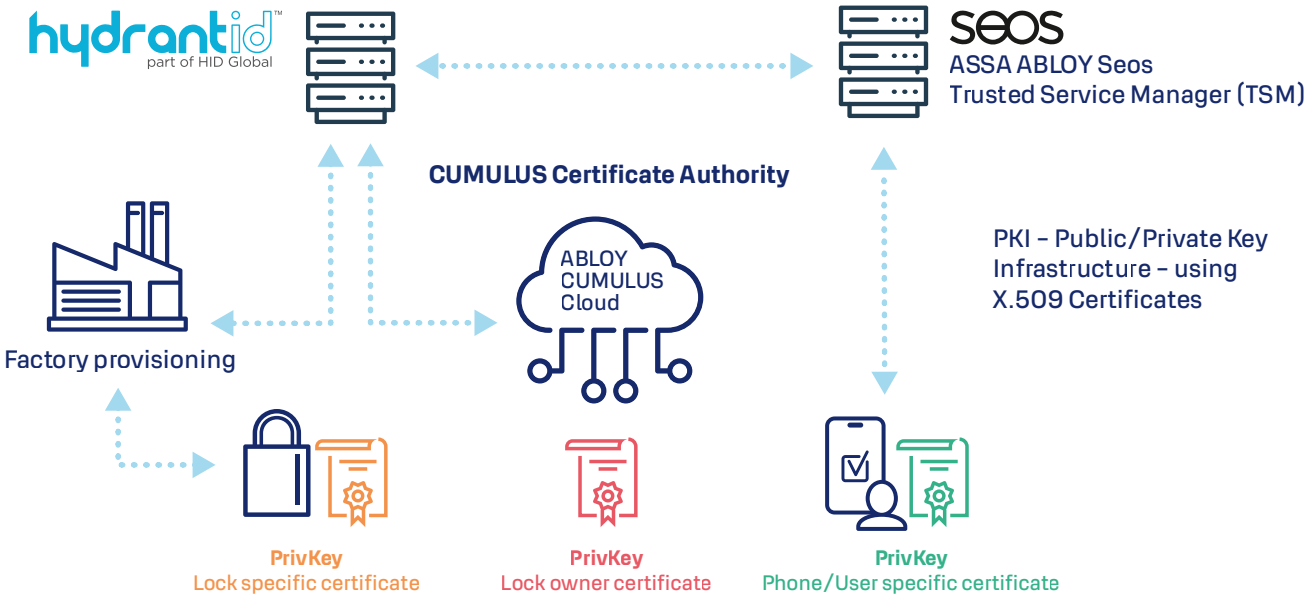
This is all part of the CUMULUS Certificate Authority system which will make sure all certificates are created and bound to a specific device according to the design and policies set.

The three main parts of a locking system

Lock – The lock gets its manufacturer certificate during the manufacturing process and is injected into the lock at the factory. The identity (X.509 certificate) is stored in a secure way and cannot be accessed or changed in anyway other than by the manufacturer if needed.

Lock owner – The organisation or operator of the lock must have an identity like we previously explained and this is represented by a certificate of which the public key is injected to each lock at the time of claiming the lock to the owner. This identity's private key is stored in the CUMULUS Cloud and is not directly accessible. It will only be used programmatically to sign access payloads. We can cryptographically give a user a specific access to a specific lock for a specific time, and we call this the access payload. The owner organisation or operator can do this through an access management system or directly through a programmatic web interface (API).

Phone/user – The users get a certificate representing their identity in the CUMULUS ecosystem. This is initiated by the lock owner by creating a single-use invite for a certain user's device. The invite is sent via SMS or email to a user's device and requires action within a customisable time period, or the link will expire. Once an invite link is used, it cannot be reused.



Cryptography

How can asymmetric locks be secure?

With the progress in technology, we now have better encryption algorithms and more processing power in devices to use more sophisticated encryption schemes. We present an asymmetric encryption scheme using the latest elliptic curve technology (secp256k1), the same technology that is used in many crypto currencies and blockchain technologies.

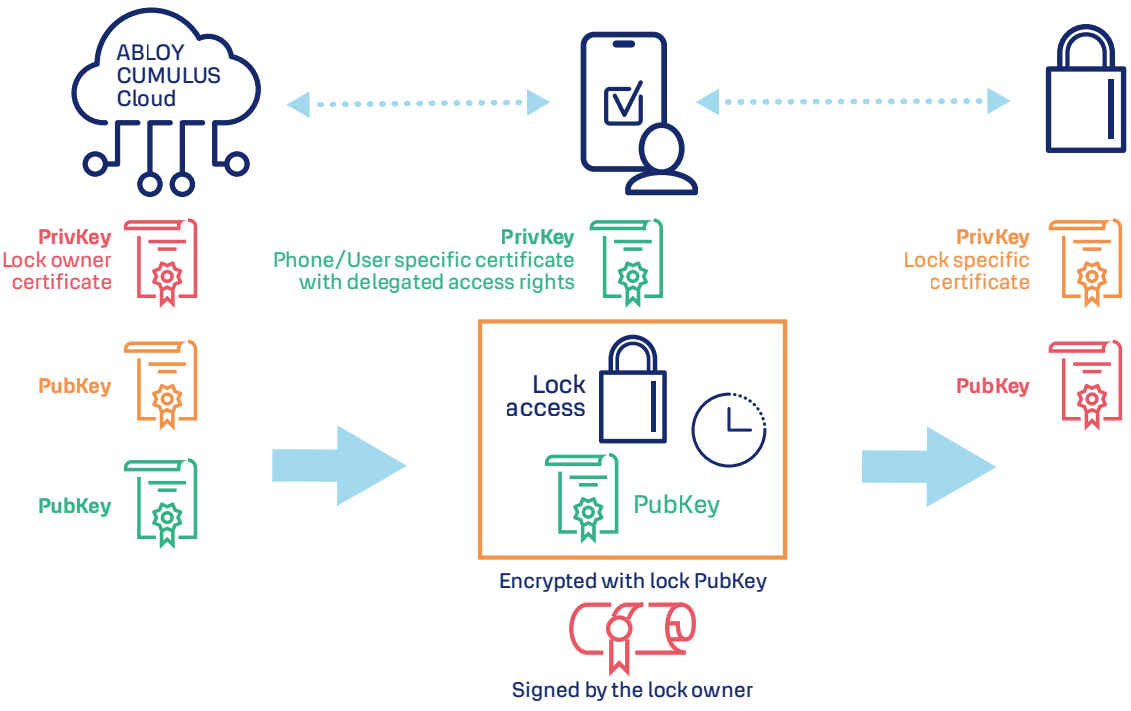
Using this very strong encryption we can give an access payload to a specific user, that is encrypted in a way only a specific lock can read. To break this down into smaller parts: since all parties have their own public and private key, we can use this to either encrypt or sign messages. Basically, we ensure that full authentication and authorisation can be made by the lock, and then grant access accordingly.

The user receives an access payload or encrypted package that consists of the user's "Public Key", a time constraint, and the command to give access to the lock. This is further signed with the lock owner's private key, so that the lock can be certain of the authenticity of the message.

The identity is stored in the CUMULUS Cloud and is not directly accessible. When the user tries to operate a specific lock, the mobile application sends the payload to the lock. The user has no visibility into the payload, which specifies the lock in question, validates user and the lock owner and defines the time window during which the access is granted. The lock will only grant access if all the requirements are met. The payload can be used for as long as the time window is still valid. The chosen cryptographic technologies and system architecture may also present future possibilities, for example single-use openings and other ways to delegate access payloads.

Security and data integrity is ensured even if the access payload would be compromised from the user's device. The payload cannot be used from any other device since the access payload is signed to only allow the single device to operate the lock.

The CUMULUS solution provisions access payloads to users. Encrypted payloads are managed in the CUMULUS Cloud. To gain access to a lock, the mobile application sends the payload to the lock for validation.



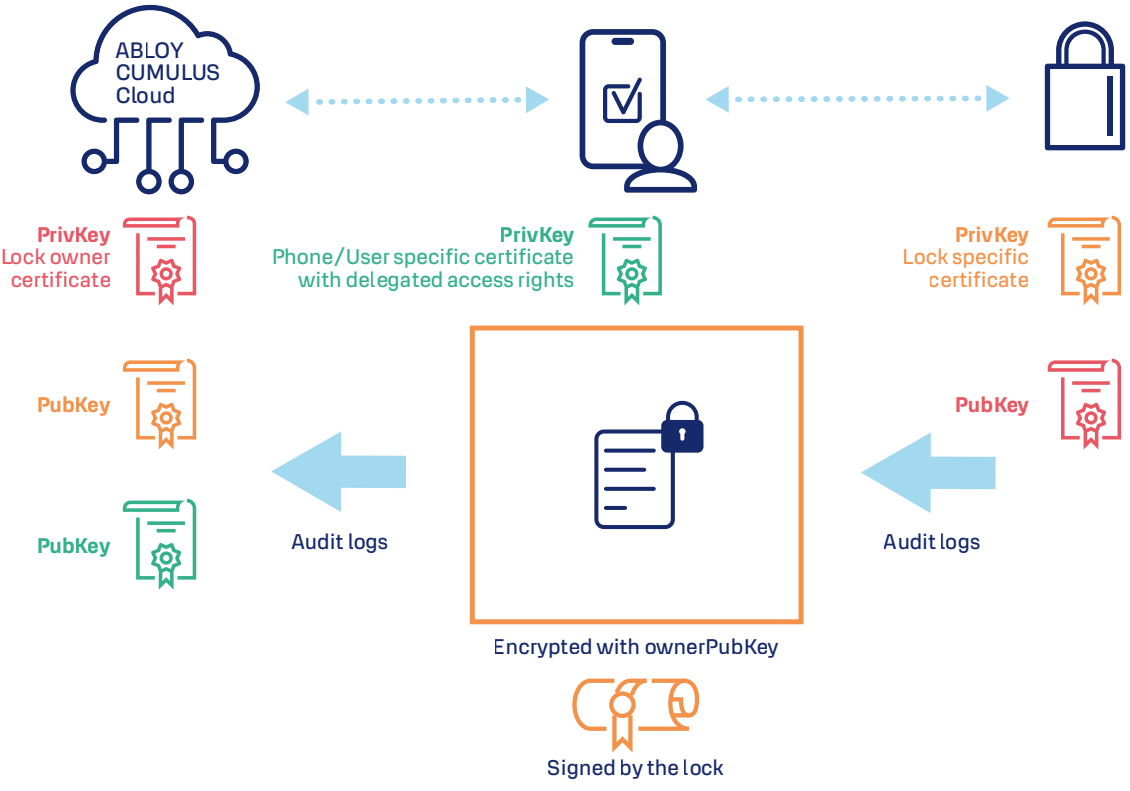
Audit Trails: offline and online

If the locks are not directly connected to internet, can audit trails be collected?

Similar to the access payload, the user's device delivers audit logs to our cloud. All transferred data is end-to-end encrypted and signed in a way that ensures there is no possibility to tamper with the audit trail. The cloud service verifies the signature and authenticity of the logs. Confirmation message of the received audit trail logs is then securely given back to the lock so that the lock knows audit logs have been transferred. If the user's device is online when operating a lock, the logs are sent immediately to the cloud.

Audit logs are saved locally in the lock in a secure way for some time. If the current user's device is offline and cannot update the audit trail, or if the mobile device is never turned back to online mode, the next online user operating the same lock will deliver all the missing logs. All users are unique in the system, so the logs can identify which specific user's device has accessed the lock and when. Each CUMULUS lock also has an internal real-time clock. This ensures each lock can independently evaluate the correct time and timestamp all the logs with the correct time.

User devices deliver audit logs to the CUMULUS cloud. If a user device is online, the logs are sent immediately. If the device is offline, the next user delivers the missing logs.



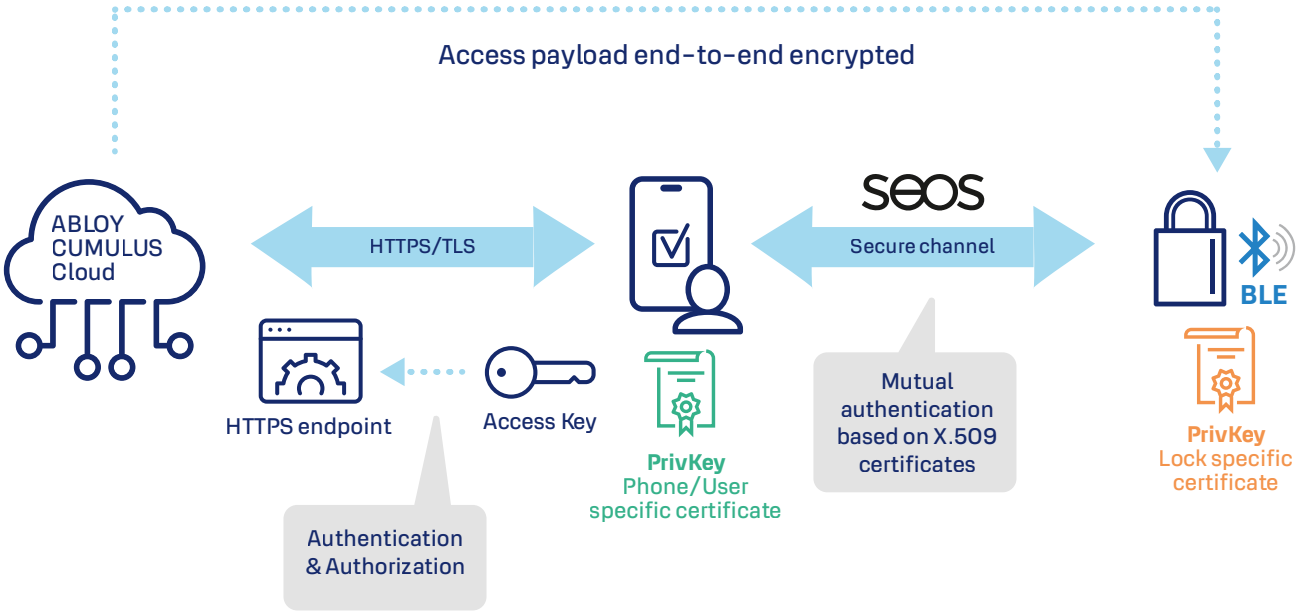
Communication

Even with a secure, end-to-end, encrypted access payload, we want to have secure communication at all levels.

In the CUMULUS cloud we have an application programming interface (API) endpoint for mobile applications. The mobile application must authenticate itself to utilise cloud services. The access credentials are given when the mobile device is invited to an organisation and added to the CUMULUS ecosystem.

The lock and phone communicate over a wireless Bluetooth Low Energy (BLE) connection. BLE connection is only used for transport and a secure Seos channel is established between the lock and the phone. Seos secures the lock's and the user's identities and strong encryption ensures that all communication and the access payload can be delivered securely to the lock.

Multilayered encryption and certificates make sure that the CUMULUS cloud, locks, and user devices communicate safely to each other.



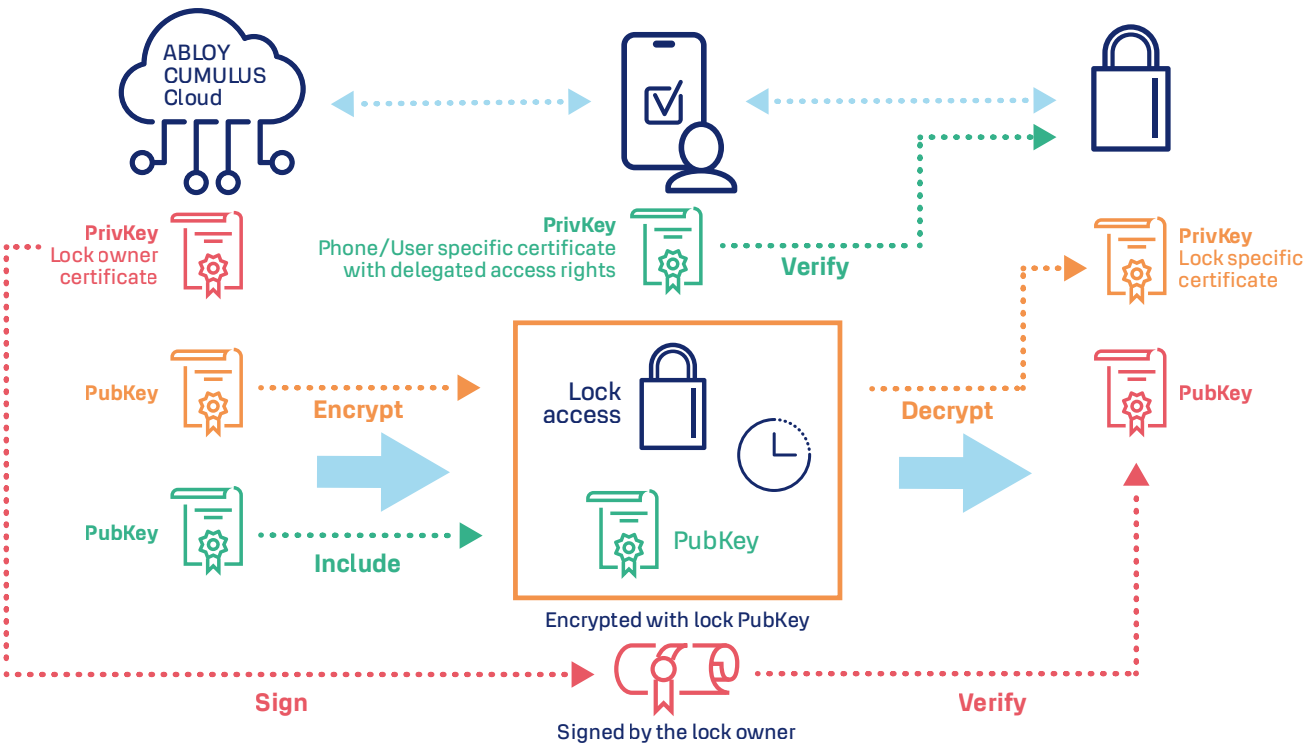
Conclusion

We at Abloy have introduced a unique solution to the market with proven technologies that follow industry-best practices. The security of this solution is as strong as any current crypto currency scheme, and as the world moves to newer technologies, we can adapt to new technologies. One might call it post-quantum cryptography.

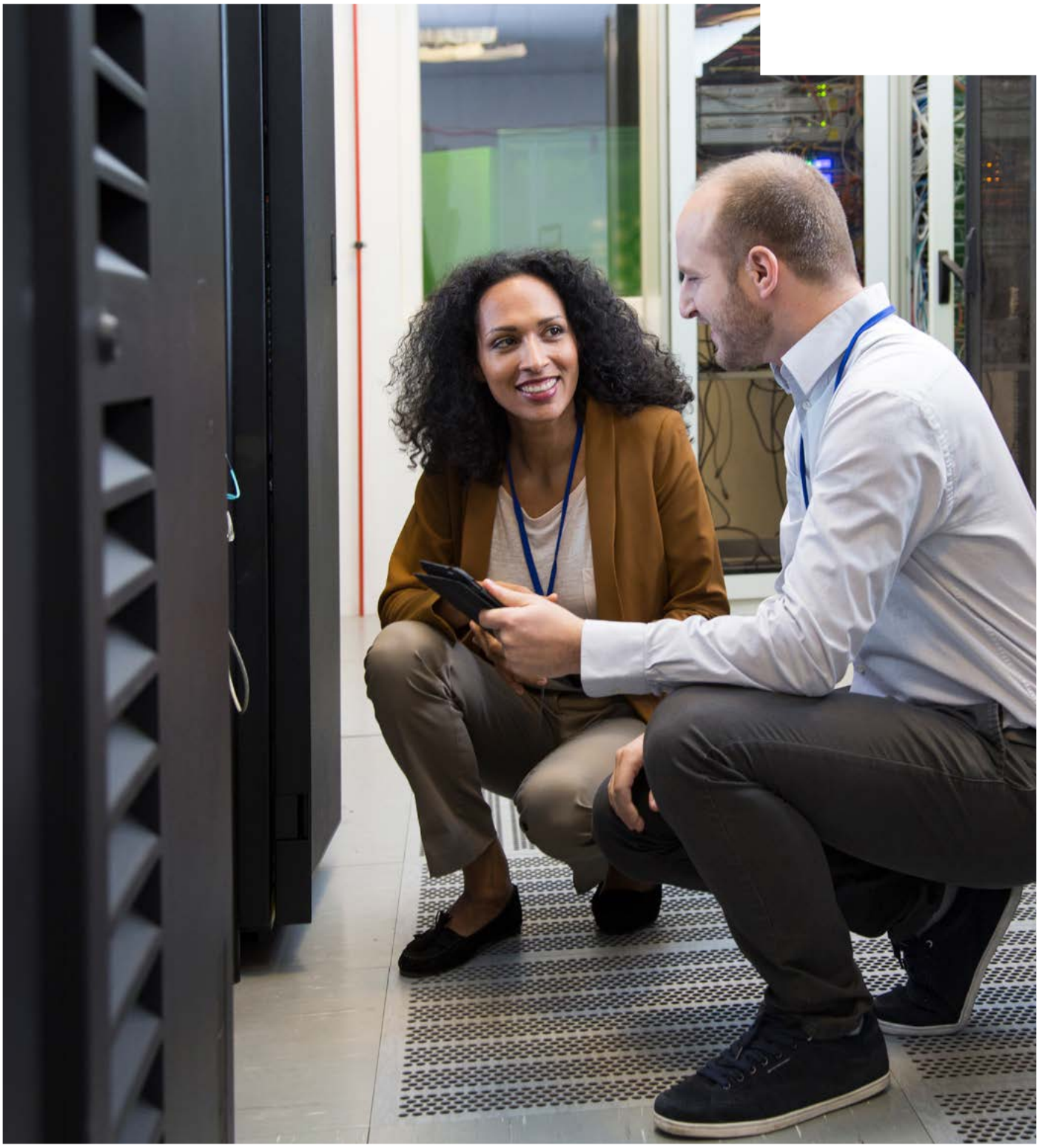
Currently, there are very few solutions using asymmetric keys for both the user and the lock in access management situations.

This solution is one of the few that does not require any provisioning of the lock for granting new access rights, and where every user still has an individual key, allowing for a full audit trail of who has accessed when and where. at all times.

For easily operable and modern security management, CUMULUS is the key to keyless access. Underneath a smooth user experience CUMULUS combines multiple layers of security measures into an integrated cloud service.




ABLOY



1/2024

ABLOY offers security and locking innovations dedicated to creating more trust in the world. Combining digital and mechanical expertise, Abloy Oy develops industry-leading security solutions that protect people, property and business. Abloy is part of the ASSA ABLOY Group, the global leader in access solutions. Every day, we help billions of people experience a more open world.

Abloy Oy
Wahlforssinkatu 20
P.O.Box 108
FI-80101 Joensuu | Finland
Tel. + 358 20 599 2501
Abloy.com

Abloy maintains a Product Security Center at www.abloy.com/securitycenter. We recommend that You check the Center on a regular basis in order to be fully informed of product security updates, so that your knowledge of our products remains optimal.

It is the customer's responsibility to define the required level of security, whilst taking into consideration relevant factors for its operations. To achieve the overall level of security required in the customer's operations multiple layers of security must be in place. These include for example locking system, key management system, access management, CCTTV and alarm system as well as physical security in a manner and level specified by the customer.

MANAGEMENT SYSTEM CERTIFICATION
DNV
ISO 9001 • ISO 14001
ISO 45001 • ISO/IEC 27001

ABLOY

Part of ASSA ABLOY