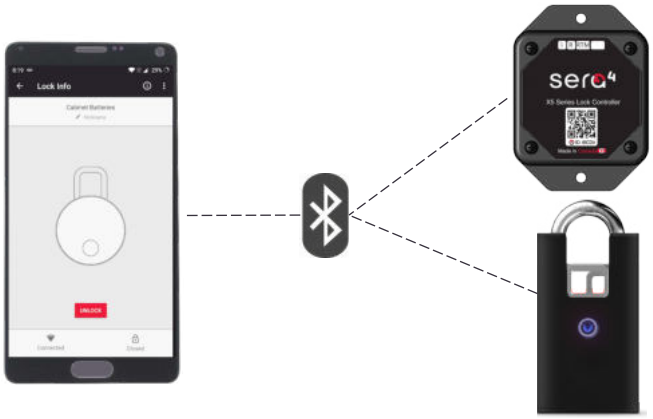
Embedded Security Padlocks and Lock Controller

Bluetooth Only as a Transport Channel

The Teleporte mobile application uses the Bluetooth radio only as a transport channel to communicate with Sera4 padlocks and controllers.



Bluetooth security mechanisms and protocols, including pairing, are not used

Asymmetric Cryptography Architecture

Teleporte uses principles of asymmetric cryptography to encrypt the communication between smartphones and Sera4 padlocks and controllers.

Private Key: Private keys are used by padlocks and controllers to decrypt information. Each controller uses a hardware-based random number generator to derive its own private key, which is never shared or seen by anyone. Even if it was possible, hacking a private key would only give access to a single lock.

Public Keys: Public keys are used to encrypt information sent by mobile devices to the padlocks and controllers over Bluetooth.

Digital Certificates: Asymmetric cryptography is also used to protect the access keys that administrators assign to users. The Teleporte server uses private keys as the root of trust to sign digital certificates with access information. These certificates can then be validated by the mobile device and the X-Series controller by using public keys.

Implementation Highlights

Encryption Algorithm

Teleporte uses a 192-bit ECDSA (Elliptic Curve Digital Signature Algorithm) standard, recommend by NIST, to: digitally sign certificates, provide authentication, and encrypt communications.

Rate-Limiting Authentication

Controllers and padlocks use time-based rate limiting of authentications to ensure they system cannot be hammered with lock codes in brute-force attacks.

Real-Time Clock

Each X-Series Controller has a real-time clock for independent time tracking. This prevents “time-based” attacks where hackers attempt to modify the validity of keys and the access log

Embedded Storage with no Personally Identifiable Information (PII)

Access logs are stored on the X-Series Controller without PII. If a malicious user were to turn off his cellular radio and avoid uploading lock logs to the Teleporte Web Services, the next user would be able to retrieve and upload those logs keeping a reliable access log registration.

Beyond Security

The benefits of this Asymmetric Cryptography architecture go beyond security as this design also enhances scalability and flexibility.

Scalability

The padlocks and controllers do not have to remember specific mobile devices - as in the case of Bluetooth pairing - nor be pre-programmed. The Sera4 solution can authenticate an unlimited number of users per lock.

Flexibility

Sera4’s patented security architecture uses asymmetric cryptography so it can be used with other radio technologies such as NB-IoT, LTE-M, Wi-Fi.

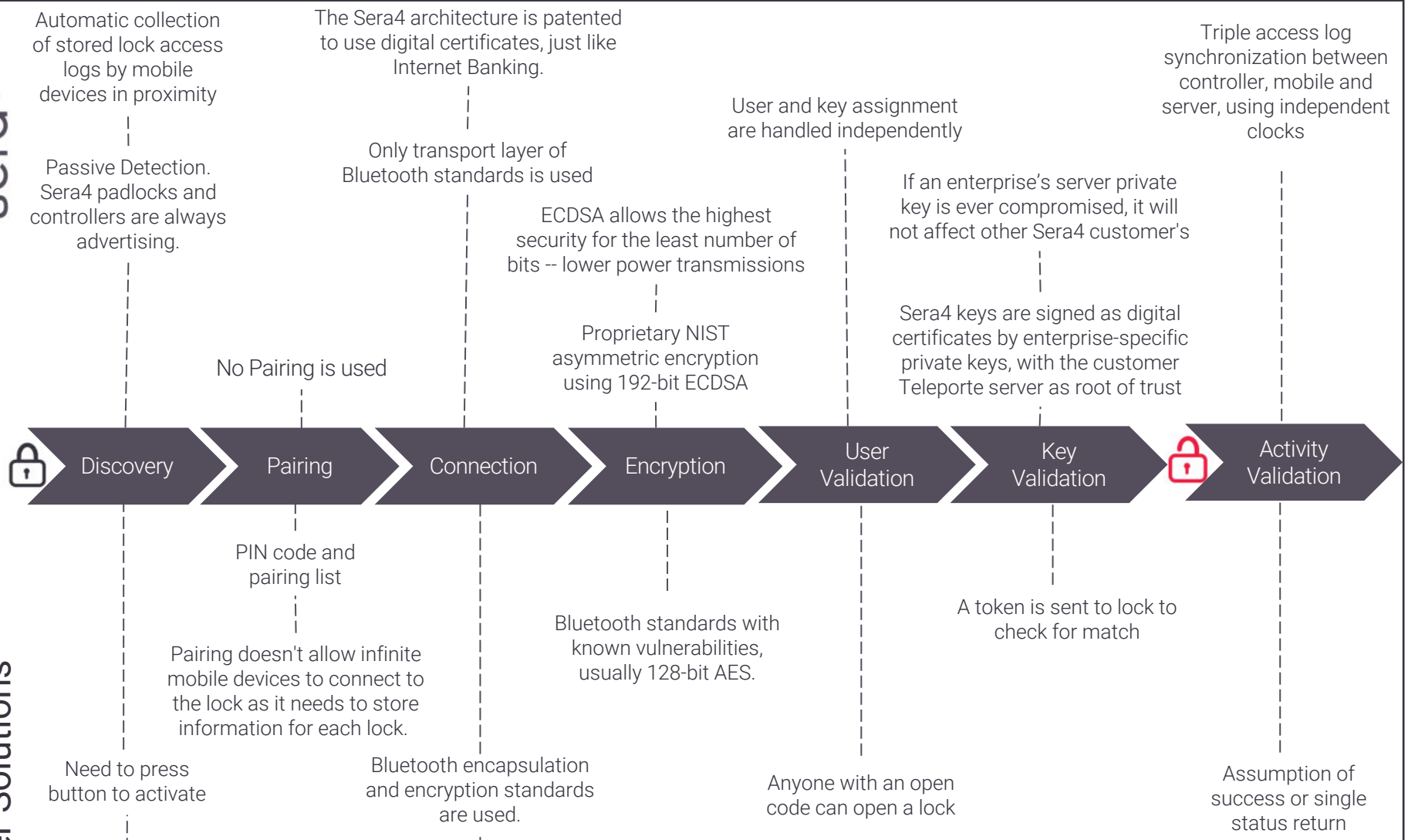
Patented Design

The patented solution from Sera4 provides a new level of security, reliability, and scalability than has ever been deployed in a keyless access control system.

US Patents 10,008,061 and 10,403,070.

For more information email us at info@sera4.com

Wireless Differentiators Padlocks and Lock Controller



For more information email us at info@sera4.com