



Custom Encryption Key Service

Smart card encryption keys

End user ownership, control and hardware interoperability

Why invest with a manufacturer who locks end users into a dated, proprietary encryption key business and technology model?

Instead, consider an investment with Schlage and our open architecture, non-proprietary Custom Key Encryption Services which provides a greater level of control and flexibility for the end user.

As a trusted authority, Schlage's Custom Encryption Key Service creates an encryption key unique to the end user. This encryption key is owned and controlled by the end user - not Schlage.

Processes and infrastructure have been put in place to transparently develop and securely store custom encryption keys on behalf of the end user. Schlage has committed to manufacture products with the end user's unique custom encryption key, without ever seeing the secret information. And, Schlage will securely distribute the key back to the end user upon request.

WHY CONSIDER OWNING A CUSTOM ENCRYPTION KEY?

- As the end user, you own the encryption key rather than the manufacturer owning the key.
- As the owner of the key, you determine which channel partners are assigned as authorized resellers of credentials, card readers and intelligent locking hardware configured with your custom key.
- As the owner of the key, you can request possession of the key and seek other manufacturers to meet your electronic access control needs.
- Custom encryption keys enable interoperability among competitive hardware manufacturers.
- End user environments, installed with a mix of manufacturers, may now be able to use a single credential among multiple hardware manufacturers.

Schlage has partnered with NXP and its globally leading MIFARE® brand to provide smart card solutions, giving our customers greater choice and flexibility when building their ecosystem. The relationship between Schlage and NXP is aligned with industry standard encryption key creation and diversification standards enabling manufacturer interoperability serving end user needs especially in mixed manufacturer hardware environments.

Schlage's Custom Encryption Key Service is designed to create control, leverage and interoperability for the end user. Interoperability extends credential utility to other hardware manufacturers aligned with this non-proprietary, open architecture model.

Schlage hardware portfolio

In most cases, Schlage Custom Encryption Keys are based on the latest MIFARE DESFire® credentials, which supports the most advanced security features and a genuinely open multi-application architecture that works natively with Schlage's portfolio of standard and mobile enabled card readers and intelligent wired and wireless locksets.

Schlage offers an easy to order channel process ensuring accurate order configurations and responsive turnaround times demanded by the market.

- MIFARE DESFire® EV2; single and multi-technology credentials
- NDE and LE mobile enabled wireless locks
- AD300 wired and AD400 wireless locks
- MT and MTB multi-technology readers
- Schlage Control™ mobile enabled wireless locks
- Schlage RC IP-based reader controller

**Please contact your local Allegion Sales Representative
to discuss, review and execute a custom encryption key for your organization.**

Or contact: ElectronicInsideSales@allegion.com

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in seamless access, with leading brands like CISA®, Interflex®, LCN®, Schlage®, SimonsVoss® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion secures people and assets with a range of solutions for homes, businesses, schools and institutions. Allegion had \$2.9 billion in revenue in 2019 and sells products in almost 130 countries. For more, visit www.allegion.com



ALLEGION™

KRYPTONITE ■ LCN ■  ■ STEELCRAFT ■ VON DUPRIN

© 2021 Allegion
013734, Rev. 04/21
www.allegion.com/us