Q. Would you explain the concept of authentication and encryption and why this creates a more secure transaction?

A. In the context of access control and the relationship between a smart card and reader authentication is the process ensuring the credential and the reader have the ability to speak to and/or communicate with one another. The credential and reader engage in a series of rapid transactions (milliseconds) and once authentication occurs the format or data written into the secure memory in a card is harvested, encrypted and passed to the card reader where it is decrypted and the data within is then sent to the control panel for the access decision to be made.

Q. Why has MIFARE DESFire not been more readily accepted in North America?

A. MIFARE by NXP was originally focused on transit applications. MIFARE innovation led to additional product developments including MIFARE Classic, Plus and DESFire EV1/2, etc. expanding utility to electronic access control applications. The NXP platform has greater share in Europe than North America, however, the last few years awareness and adoption of EV1 and EV2 is incrementally growing in the North American market.

Q. What is LEAF?

A. LEAF is a consortium of NXP aligned credential and hardware manufacturers driving an open, interoperability standard enabling the use of a single credential to be used among multiple manufacturer hardware platforms. Visit the LEAF website to learn more: https://leafidentity.com/.

Q. What is a key sharing ceremony?

A. When the owner of a custom encryption key decides to share the key with another entity the key is optimally shared via a secure key exchange ceremony. Multiple key sharing options exist and standards have been developed focused on the transparent and secret sharing of keys. An element to key sharing too is the risk associated with sharing the key, how the key is stored and protected post-ceremony and the liability associated with secure key storage.

Q. If I think I'm in a proprietary credential relationship, but prefer a more open solution like you have explained with MIFARE DESFire, what are my options?

A. Please contact Allegion InsideSales@allegion.com or Paul.Iverson@allegion.com at 303.882.7539 or your local Allegion Sales Representative.

Q. What if I want to own my key, but don't want to secure it. Is there an option where Allegion can still safely hold it even though I as the end user own it?

A. Yes. Allegion will develop a key for you and provide the secure storage of the key as well. As the owner of the key you will assign Allegion the rights to securely store the key.

Q. Why would I want a proprietary model (as an end user)?

A. If you're comfortable with the manufacturer's portfolio offering, the roadmap and the channel fulfillment and pricing strategy the proprietary model may be a good option for your situation.

Q. Have you run into any situations where a low frequency prox card was duplicated for theft purposes?

A. Have not witnessed the copying of a card for theft purposes per se. When a card is cloned the end user customer is typically not aware this has occurred and more than one copy of a credential, assigned to the same person, is being used. One way to determine if this has occurred is if one copy of the card were used at one location and another copy of the card was used at another location within a timeframe where it is not physically possible for the user to be in those two places. I have however, for demo purposes, cloned a customer's card and showed how easy a card is to replicate. The demonstration is powerful.

Q. Is there a user license for an end user owned encryption key? What is the cost? What is the cost if I stay with the proprietary version?

A. There is no user license to provision a custom key. It is a one-time cost. The part number is SCEKS and pricing is available through the channel.

Q. Would Allegion be willing to provide cards only for a project?

A. Yes, please contact your local Allegion Sales Representative.

Q. Are Allegion and HID compatible?

A. Yes, on a limited basis at this time. Allegion's AD 300 and 400 hardware offer an option to support the iClass and SEOS encryption keys. Even though competitors we do work together to address shared challenges in the market.

Q. So, an Allegion Card Reader can read any MIFARE Classic, MIFARE DESFire, etc.?

A. Yes – the Allegion portfolio of Schlage readers and electronic locks can support a variety of DESFire technology including MIFARE Classic, MIFARE Plus and MIFARE DESFire technologies.

Q. Other than just standard 26 bit format, what other bit formats are acceptable with Schlage Control locks?

A. Yes - the Allegion portfolio of Schlage readers and electronic locks can support a variety of bit formats including but not limited to 26A, 35C, 37X, 40X and 48X. Overall, Schlage readers and electronic locks can support smart credential bit formats up to 63 bits.

Q. How does NXP technology interact with the iClass technology from HID?

A. When talking about smart, high frequency technology, NXP MIFARE and HID iClass are two different technology platforms and do not transact with each other. To support NXP or HID technology a manufacturer must have the corresponding technology and the correct symmetric key on their reader.

Q. What is the status of EV3 cards and readers? Mass production, limited production or will be available soon?

A. NXP publicly announced the introduction of MIFARE DESFire EV3 in June 2020. Allegion is currently working to transition all DESFire EV1 and EV2 smart credential technologies to DESFire EV3 by the end of 2021 if the supply of EV3 chips are available.

Q. Will this work with then new HID Signo Readers?

A. It is always recommended to check with the manufacturer on their support of various technologies, but based on publicly facing documentation HID does offer NXP technology support on their Signo readers if the right configuration is chosen.

Q. I understand the benefits of MIFARE DESFire encryption. I do not understand all of the option pertaining to memory? (1K, 2K, 8K, etc.) Can you explain?

A. NXP offers their different technologies with an option of various memory sizes. You can think of these chips as mini-computers or a smart cell phone that stores data and can make calculations. These different memory sizes allow for the customer to determine how much memory they might need to support the function they wish to use the cards for in the market. The higher the memory, the more information can be stored before the memory is full. The less memory, the less data can be stored. For basic access control, 1K or 2K memory is plenty of memory to support basic programming information. If you want to leverage the card for access control and other uses such as dining or transit, more memory, such as 4K or 8K might be needed.

Q. Do you know if the ISONAS readers read the custom credentials you're talking about today?

A. ISONAS readers are based on NXP technology and can support custom keys.

Q. If the MT15 reader is wired in OSDP, can the command to turn off the 125 kHZ range and just leave EV2 on be sent via the OSDP/Access Control software, and not use config cards?

A. Allegion follows the SIA OSDP specification to support configuration updates via OSDP. It is critical to make sure the product you are ordering has RS-485 capability. The Schlage MTB series comes with RS-485 standard, the Schlage MT Series -485 must be specified. In addition, the software provider and panel provider must also support OSDP to push configuration updates.

Q. What mobile formats do you use?

A. The bit formats supported on Allegion mobile solutions vary depending on the solution. We continue to add more bit format support. In general, our Student ID NFC solution supports 35C and 40X and our Schlage Mobile Access Credential supports 26A and 48X.

Q. Does Allegion have any tools to assist customer in creating their own keys and transfer those securely to Allegion? Is there a tool that demystifies this complex subject?

A. Allegion does not currently have a tool to assist customers in creating their own keys, but Allegion can securely create a custom key for the end user to own. In addition, Allegion is building out tools to securely receive custom keys created by others in a "zero trust" manner.

Q. Is Allegion looking at PKI for future encryption or are they planning to stick with symmetric keys?

A. Allegion is looking at and considering PKI models, specifically for mobile credentials.

Q. Any concerns with long lead times of MIFARE DESFire EV1 and EV2?

A. There is a global chip shortage driving long lead times for smart credential chips. Allegion has a dedicated team who is working diligently to mitigate this risk and minimize the impact to our partners. Today we are still able to provide standard lead times on our MIFARE DESFire credential portfolio.