What is PKOC ?

Everything that you wanted to know.

Jason Ouellette – Elatec
Ed Chandler – SBD

TOC

QUESTION 1 - What is PKOC?

Public Key Open Credential (PKOC) is the best development that has come to the access control industry in many years.

- Security
- Cost
- Simplicity
- Interoperability
- Globalization

PKOC is a publicly available specification for access control credentials that is defined with two methods of delivery:

- An NFC specification can be used for access cards or, in the future, mobile devices
- A Bluetooth specification that can be used for mobile devices
- These two specifications have been created by the Secure Credential Interoperability (SCI) Working Group of the Physical Security Interoperability Alliance (PSIA) https://psialliance.org/

PKOC's design is based on industry standard X.509.

- PKI stands for Public Key Infrastructure and PKOC utilizes a portion of PKI that is better stated as PK, or PKI without the I.
- The only key that is shared is the public key.
  - The public key is the credential, just like any present access card number.
  - The access card number needs to be available to put into an access control system.
- X.509 is a process that defines the creation of a key pair, a public key and a private key.
  - The public key is shared as the credential number.
  - The private key is never shared. It is stored in a vault of the device where it was created.
  - The public key and the private key are different, thus asymmetric keys.

PKOC is open.

- No manufacturer "owns" this technology.
- It is owned by the industry, donated through the efforts of PSIA's (SCI) Working Group.
- Any reader or card manufacturer can make and market PKOC readers and credentials with no license fees, royalty, or membership required.

PKOC is simple, free from complexity.

- The public key is the credential number.
- No Facility code, site code, issue code, or other data element needed for uniqueness.
- One decision that must be made is based on the capabilities of the existing access control system; that of the bit length that will be used for that system. See "more" below for the explanation of this.

Question 2 - What is the unique value of PKOC?

PKOC credential security is extremely high.

- The encryption is asymmetrical.
- Almost every other physical credential in the market today is symmetrical.
- Even those access cards that are listed as “high security” use symmetrical keys.

PKOC costs less than other credentials.

- No organization can utilize pricing advantages because they are the sole source.
- The market will manage PKOC pricing because it is open and not owned by any one entity.

PKOC is simple.

- In the access control system, choose to use a bit length for the credential.
- No facility code, issue code, site code, etc. is required for set up.
- No complex card format and bit set up.
- No card number to keep track of when ordering or added cost for a service to do this.
- No worrying about duplication or cross access from other facilities.
- No key to share for readers or card to be manufactured.

PKOC is interoperable.

- A great example of the beauty of PKOC is a multi-tenant building with building security.
  - The building can utilize PKOC readers for the perimeter doors, turnstiles at the lobby, and elevators to allow tenants access to assigned floors.
  - The tenants can have PKOC on their access card or in their mobile device.
    - Tenants can use PKOC as their access credential
    - Or, tenants can use their present older, less secure, credential from any of the common credential suppliers, assuming that they also have PKOC in a multiple format card.
    - Since the card or mobile device always provides the full public key (single source of truth), different tenants can use different lengths of the PKOC credential and still have full interoperability with a single credential.

PKOC can be a global solution.

- Outside of the US, there are common credentialling solutions that are uncommon in the US.
  - It is possible to source NFC access cards with multiple credential types, including PKOC, at reasonable card pricing.

Question 3 - Who benefits with PKOC from a security perspective?

End Users
Ultimately, it is the end user that benefits the most. This starts with the security enhancement of moving from Symmetric based credentials to a higher security Asymmetric encryption credential.

The access control industry has matured their offerings over many years, taking advantage of the developments in small, low power chips that can do simple things. Now, with widely available and low cost JAVA chips, PKOC will revolutionize the credential in a card. Additionally, all smart phones today already have the capability to create and use a PKOC credential.

PKOC is an asymmetrical PK process. All other common card/reader technologies on the market are symmetrical. The difference between the two is uncalculatable. With PKOC, a public key – private key pair is generated in the card or mobile device. The private key is kept in the card's private "vault" and the public key is shared as the card number. If someone were to find a way to compromise that key pair, the damage would be 1 card. But that compromise would signal a monumental change in how cyber protection succeeds today. PKI and X.509 certificates are the fundamental and underlying basis of cyber protection today.

Manufacturers
Manufacturers benefit from the fact that the larger view of the access control system is more secure. The various hacker conventions will need to focus on other areas of interest because the attack surface of the access card is 1. The change to PKOC will be the most significant security upgrade in access control in many years.

Integrators
Integrators bring system opportunities to customers in many ways. Their ability to provide cost effective security enhancements helps market their value to end users.

Consultants
Security consultants now have a tool in their offerings that does not have the vulnerabilities that are caused by the wide use of symmetric keys. Before PKOC, the only major offering that used asymmetric keys was PIV and the commercial variant CIV. But PIV and CIV, as an architecture comes with the I, meaning the Infrastructure of a centralized Certificate Authority (CA) cost, complexity, and management burden.

Question 4 - Who benefits with PKOC from an interoperability perspective?

End Users
If you are an end user with just one site with a suite on a floor of a multi-tenant building, the likelihood is that you will be using the building's card and reader types even if you have your own physical access control system. But if that is not the case, and your cards are different from the landlord's cards, your employees will be carrying two cards. The exponential growth of this problem, as an end user adds more sites, quickly becomes untenable.

Integrators
Integrators are the entity that must deal with all the variations of legacy card technologies.

- Even with the latest symmetric card technologies, there are size and format options that need to be considered.
- The access control system must be configured for the right credential bit size, format, and facility code.
- The symmetric keys may be widely available with an off-the-shelf generic secret key or a secret key that is assigned to a single end user.
- This affects the ordering process when adding to a card population.

Manufacturers
The manufacturers benefit from a lower complexity and faster time to market. With real interoperability comes less need to support the near 80+ common card format and reader types in the market today which reduces development, testing and improves the quality of the products they bring to the market.

Consultants
Large organizations, by their very size, have facilities in multiple areas. Often some facilities are relatively smaller offices that lease space in multi-tenant buildings. Some of these multi-tenant landlords are becoming aware of PKOC as an open interoperable technology opportunity. A PKOC credential could be implemented throughout an organization's Real Estate and that same PKOC credential could be used at the public locations of a multi-tenant facility. These locations could be parking, building main entrances, privatized restrooms, lobby turnstiles, and elevators, both typical in-cab reader controls or a Destination Dispatch system.

Consultants will have one more reasonable option to design interoperable systems.

Question 5 - Who benefits with PKOC from a cost perspective?

End User
The end user ultimately benefits with PKOC from a market that is less complicated and free from proprietary product offerings. Integrators will save money by not having to deal with all the issues that symmetric keys encompass, and at some point, those lower costs will show up in integrator pricing.

The open and publicly available specifications for PKOC allow any entity to enter this market. There are no restrictions, and no licensing fees, royalties, or memberships required for proprietary products.

Integrator
As the PKOC market matures, more individuals that set up and program access control systems will find that PKOC is less complicated.

- Reduced complexity
- Applicable to a wide range of access control systems

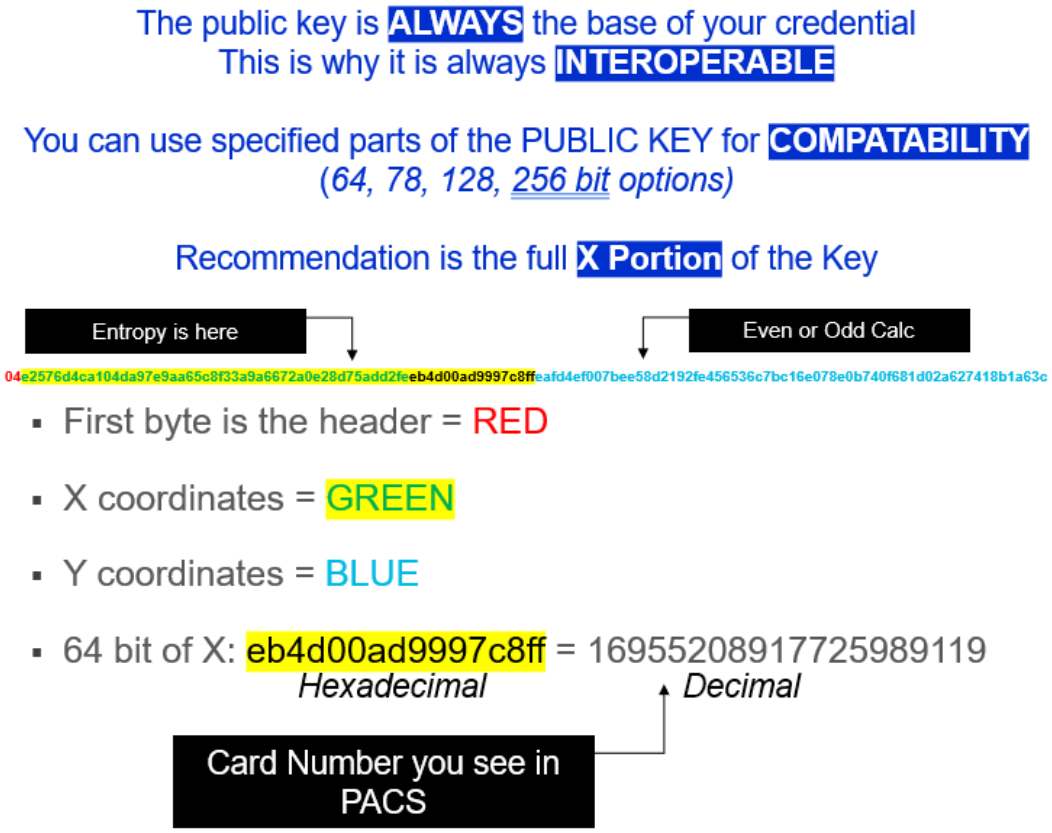
Manufacturer
The manufacturer benefits from PKOC by reducing the format complexity and compatibility matrix for testing that lowers their overall manufacturing costs and improves profit margins. Manufacturers often end up with their service department managing the complexities of GUIDS, bit length, facility codes, and other symmetrical key credential issues.

Consultants
Consultants support end users with more than just physical system designs. There are all the other complexities that come up where the end user has a challenge and needs a translator and support person. Consultants are not always in a good position to monetize these peripheral activities.

Question 6 - How does PKOC work?

The card
PKOC credentials can be made with many OSs like JAVA, Unix, Linux, and Microsoft Windows. Mobile phones and JAVA cards are the most expected users of PKOC. JAVA cards are widely available and inexpensive. Any PKOC credential that meets the specification will work with any PKOC reader that meets the specification. It is up to the management of the Access Control System (ACS) to put valid credentials (portion of the public key) into the ACS. And, if that credential is no longer needed in the ACS, to deactivate that credential or remove it from the system.

The public key is actually 65Bytes (520bits). With Elliptic Curve Cryptography (ECC), which is used for PKOC, all or a portion of the X information within the 65Bytes can be used as the credential.



The description of the process for a PKOC card read is in the More Technical Information for Question #6.

Question 7 - Why is there no need for a centralized key management system?

A centralized key management system with asymmetric key pairs utilizes a Certificate Authority, and usually sub CAs, to create and distribute the keys. The ability to create a CA is built into every Microsoft OS. Setting up a good secure CA is not a task for the uninitiated. The underlying vision of PKOC is to not require a CA, not require any centralized management, but to simply use the X.509 key pair to create key pairs on a card or mobile device and use the public key as the credential. This is the epitome of BYOC (Bring Your Own Credential).

A PKOC card can be purchased independently and brought to an organization that has a need to provide credentials for personnel into an access database, but that is not the goal. The goal is to allow an end user to purchase PKOC cards or to use software to create PKOC credentials on mobile devices. Then personnel can present this PKOC credential for enrollment at any facility which supports PKOC.

A PKOC credential is an entity in itself. It is created with commonly available code, under a standard X.509 process, and ends up with a key pair, one public that can be shared and one private that does not every leave the device where that pair was created, either a card or a mobile device. It is also possible to create a PKOC credential on other devices, but the actual use of other devices for access control seems remote. There is just no need for a distribution control system, like a Certificate Authority (CA), to manage or control these PKOC cards. Therefore, it is like PKI without the I for the Infrastructure.

Access control managers are so used to managing systems using symmetric keys that it is difficult for many to see how the PKOC environment works. There is no need to control key numbers to make sure that there are no duplicates. All the other attributes of the symmetric key utilization that could be considered “work arounds” for the symmetric systems are no longer needed for PKOC.

Question 8 - Should there be a worry about card uniqueness?

Key pairs are generated using processes defined by X.509 and are generated on the card or mobile device. There is no outside influence on this process and no “keeper of the keys” in this process. Is it possible that two public keys that are generated by two independent processes manage to come out with the same public key? The answer is yes. For a 128bit length public key usage, the chances are 1 in 340,282,366,920,938,000,000,000,000,000,000,000,000 of a duplicate.

There is a randomizer in the X.509 process that assures that keys that are created have a high likelihood of being unique.

With a system where X.509 is used within a CA, the CA will assure uniqueness. It is fair to say that, in the absence of a centralized certificate management system, it is not impossible that a duplicate public key might exist. PKOC depends on the overwhelming probability of no duplicates.

When a 64bit public key read is used, the chances of a duplicate are 1 in 18,446,744,073,709,600,000.

NO ADDITIONAL DATA IS REQUIRED

Question 9 – How can a user get access to a door? (Card, BLE, Wallet)

Once your PKOC credential is enrolled with a PACs or IDMS, access levels are assigned to the credential and used to either grant or deny access to doors when presenting a PKOC credential. This is the exact process that ACSs have used for many years. There is no difference when using PKOC.

Is there a difference in the speed of the card read with PKOC? Not really. There is a bit more work being done in terms of moving data and the size of the data. But tests show that card reads are still sub-second, with typical reads from the time of card presentation to the unlock relay on a panel to be about 500 milliseconds, or ½ second.

The only other asymmetric access control system that has many users is PIV. That system definitely has infrastructure, so PKI is appropriate. PIV access reads run between 2 to 4 seconds, feeling very slow to the users.

NO ADDITIONAL DATA IS REQUIRED

Question 10 - What to specify for a PKOC system?

PKOC readers that meet PSIA's specification, including the AID, for complete interoperability.

- The sources for PKOC readers are limited at the time of this initial publication in 2024. However, there are multiple sources that are working on PKOC readers that will be in the form factor that the US market is familiar with, specifically switch plate size and mullion size readers.
- SBD and JCI have tested several PKOC readers and more will be available soon.
- For securing the communication channel between the reader and the panel, use OSDP Secure Channel readers.
- For older panels, if they support at least 64bit credentials, it is possible to use Wiegand communication.

PKOC access cards that meet PSIA's specification, including the AID, for complete interoperability.

- These cards can be purchased with a wide range of access control credential types as well as the PKOC credential.
  - Any good card supplier will be able to provide PKOC credentials.
- These cards can have logical access software as well, like FIDO2.
- The ultimate FIDO2 card from Sentry has a built-in biometric so that this credential is all that a person needs to meet the biometric part of the process and virtually all privacy requirements as well.

Make sure to align the bit length of the readers with the settings in the ACS panels.

Tools that are available to a consultant to use in a PKOC design:

- The specifications on the (https://psialliance.org/securecredentials/) for NFC and BLE

The specification for PKOC over OSDP is also available but you should verify that the PKOC reader you want to use can support OSDP as this is a newer option for the specification. (https://psialliance.org/securecredentials/).

See the More Technical Information for Question # 10 for details and additional files.

Question 11 - How should a consultant design and specify PKOC?

PKOC, just like any other access control system, utilizes some form of a credential and readers that can read the credentials. Since this document is focused on PKOC, the design and specification of the credentials, readers, and interface to the access control panel is the primary area to be addressed.

Greenfield
Greenfield opportunities for medium or large system designs don't come along very often. Most organizations of any size today are already using some form of access control with symmetric key credentials. But if there is a greenfield design needed, there is a great opportunity to start off without building in any of the legacy symmetric challenges that will be found in virtually all the brownfield designs.

For a greenfield, cards can simply be PKOC cards. These cards can be sourced at end user costs of less than $5.00 in reasonable volumes. Today, on Amazon, you can purchase a PKOC card, Quantity of 1, for $10.00.

The cards, readers, and ACS panels need to work together. Probably the biggest consideration is the size of the credential and how that is implemented in the access control system. Even the minimum reading of a 64bit credential number is long and the use of a wedge reader or other methodology for the enrollment will be very useful.

Brownfield
Most opportunities for the implementation of PKOC will be brownfields. There will be one or more existing card technologies already in place. Both PROX, at 125KHz, and high frequency, 13.56MHz, are likely to be found. Mixing multiple technology readers and multiple technology cards is not wise. It is much better to do one or the other. Multiple technology access control cards have been tested and they are a viable option.

While it will be possible to source readers that support multiple technologies, it may be unreasonable to assume that there is a way to get every reader in the brownfield changed before a PKOC only credential will be able to work everywhere. It will take some time to replace every reader, likely years on a large system.

With an organization that might have tens of thousands to hundreds of thousands of badged personnel, it might be reasonable to assume a time frame of ½ a year to plan and implement a total replacement of the credential for every person. That is likely a lot shorter time span than the reader replacement for the same system.

Question 12 – How should a consultant plan to migrate an existing card environment to PKOC?

If the consultant has an end user that is using a particular technology like Seos or EV2, or even PROX, what are the considerations for the process of getting to PKOC? Here are the first questions to consider given the likelihood that all readers and credentials will have to be touched when moving to PKOC or other solutions that enable wireless communications:

- 1) What security problems will you have solved by going through this transition? Are you just improving a credential experience or are you solving problems and improving security overall for the investment / efforts.
  - PKOC moves from Symmetric to Asymmetric encryption improving overall security above most solutions offered in the market today. It also frees you up from proprietary technologies that can de-risk future issues with vendors, supply chain, and preferences.
- 2) During the transition from existing technologies, how do you minimize the impact to personnel for access control while not having to replace all readers / credentials overnight?
  - Using multiple technology readers and/or credentials can allow for transition over time with minimal impact to personnel.
    - Use multiple technology credentials for a complete rebadging of all cardholders and, once that is complete, replace readers on a reasonable and flexible schedule.
    - Use multiple technology credentials for new issued personnel credentials that can work on both new and old doors so re-badging doesn't have to happen for everyone in a short period of time. Some security environments have a re-badging mandate over time.
    - OR
    - Replace readers with multiple card formats that can read both new PKOC and the existing card formats over time to ease the upfront capital costs, and then rebadge when all readers are multi-format.
    - The security problem with the multi-technology reader approach is that the final state of the system leaves old weaker technology in the reader and is dependent only on the panel configuration for security. It is recommended that you have readers that can disable the older technologies once the migration is complete.

Question 13 - When and how would PKOC be available as a wallet product?

Wallet is more aligned with the concept of an Identity. The wallets can store credentials. PKOC is just a credential. Think of PKOC as a card number.

PKOC is not supported by Apple today but could be supported by Google Wallet. PKOC will be processed in the near future with Apple's credential program by either JCI, SafeTrust, or Elatec.

Any reader that is PKOC and ECP2 certified can be used with Apple's wallet once PKOC is approved for the Apple Wallet.

Question 14 – What is aliro?

aliro is a newly announced standard from the Connectivity Standards Alliance (CSA) which also uses at its foundation a Public Key as credential. CSA has not published this standard yet, and that is not likely to happen before early next calendar year. Until then, you must be a CSA member in order to get details about what aliro is. Public information can be found here: The Connectivity Standards Alliance Announces Aliro, A New Effort to Make Mobile Devices & Wearables Central To A Digital Access Future - CSA-IOT.

Aliro represents four key principles for mobile device and access reader manufacturers, and has benefits that extend to a wide range of stakeholders, from system owners and installers to property owners and managers, homeowners, and renters, and more. These include:

- Simplicity – Lower barrier to implementation by reducing complexity for integration and streamlining troubleshooting.
- Flexibility – Supports different types of installations or architectures, offering convenient access to both common and individual entry points.
- Security – Foundation to implement state-of-the-art secured and trusted mobile access solutions.
- Interoperability – Standardized communication protocol enables manufacturer-independent devices and readers to work together at the door.

Details on aliro can only be shared with CSA members.

NO ADDITIONAL INFORMATION IS AVAILABLE

More about Question 1 – What is PKOC?

Mobile
For a mobile environment, the PSIA website has a free and public specification that defines how to create a mobile application that utilizes Bluetooth to interact with a PKOC Bluetooth reader. It also defines how to create a Bluetooth reader in terms of PKOC.

Mobile devices for years have been able to create “public key / private key” key pairs. The mobile PKOC application will work with the mobile device’s system to create a key pair. The private key will be stored in a secure vault on the mobile device. The public key will be available to be shared as the credential for access control.

NFC Card
The generation of a key pair on a card is possible due to the command set of the JAVA operating system that is available on a standard JAVA chip card and the support of ECC P-256. These cards are widely sourced and available. If PKOC is the only credential that the card needs to contain, the process is relatively straightforward. Multiple manufacturers today can source PKOC cards for very reasonable prices.

If multiple credentials are required on the same card, the effort to create more than one credential type, both of which are 13.56MHz (often called high frequency), is a bit more involved, and that will be discussed later in this document in question 4 – Migration.

PKOC is a Specification, not a Standard
Public Key Open Credential (PKOC) is a specification that provides a secure way of using asymmetric encryption. The public key portion of the key pair is the credential. It should be noted that while PKOC is a specification, it is based on the same PK standards used by most asymmetric encryptions options used today for banking, retail, etc.

PKOC does not require a royalty or special license to be utilized. It is truly open for all that want to utilize the specification. There is no concept or requirement of a member for PKOC. In today’s security industry, the openness of PKOC is a major differentiator. Today, for access control cards and readers, the industry largely relies on symmetric encryption for credentials where there is no feasible way to protect the integrity of the cards other than symmetric encryption. This means that the same encryption key must be in every reader and every card of a working group. Two examples of a working group technology would be an HID Seos Elite or a Desfire EV2 set of keys and readers where the symmetric key is unique to a “customer”. Note that there are also generic cards and readers that are generic and very widely applied which poses a very large possible attack surface.

PKOC is Simple
PKOC does not come with all the complexity with symmetric keys which use facility codes, card configurations, the need to keep track of the issued card numbers, etc. The PKOC public key is simply just a large number.

An asymmetric option that exists today, such as PIV/CIV based credentials, are centrally managed, with certificate authorities use for key distribution. This allows for key revocation across multiple environments, where the key is revoked, irrespective of the permission revocation in a system. While key revocation has value in an environment like the U.S. Government, it has been considered too complex for general application to access control.

Public Key Open Credential

PKOC, pronounced /ˈpēˌkäk/ (like peacock) is the acronym for Public Key Open Credential. PKOC represents an openly available specification, written and supported by the Secure Credential Interoperability (SCI) Working Group of the Physical Security Interoperability Alliance (PSIA) https://psialliance.org/. The specification defines a highly secure, access credential solution designed to enable interoperability. The specification is posted here at (https://psialliance.org/securecredentials/) with the intention to make it readily available to end users, manufacturers, integrators, and virtually anyone who wants to develop an app with a self-generating access credential or develop a device (reader or panel) that will consume the highly secure credential for physical or logical access needs.

This highly secure credential option will put the control back into the hands of the security practitioners. Conforming to the IT Industry Standard for Public Key cryptography, PKOC is agnostic to the transmission method, whether it be NFC, BLE, UWB, or whatever new transmission technology exists down the road, and is fully compatible with iOS and Android devices as well as Java chip access cards.

No person or entity owns PKOC because everybody owns PKOC. It is truly an Open Credential for all to use.

Future Structures
A third specification produced by PSIA is based on the same mobile or NFC cards, but can take advantage of moving the PKI work up to the panel from the reader. By moving the cryptography work to the ACS panel, it makes the work of the card reader one of transmission medium translation from Radio Frequency (RF) to electronic signals using OSDP. No part of the cryptography is accomplished in the readers.

This technology has been proven to be viable and fast in the lab, but is not available in the market as of late 2025.

More about Question 2 - What is the value of PKOC?

High Security
Asymmetric keying is the basis for virtually all cyber today. ECC, or Elliptic Curve Cryptography is the fast and very secure version of asymmetric keying and is what is utilized in PKOC. It is attractive for mobile and cards where processing power is low, and data transfers are high. Additional information is easily found on the internet. One link is https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes#:~:text=While%20AES%20is%20a%20symmetric,for%20optimal%20security%20and%20efficiency .

Cost
Anytime a market has a protected environment or secret, there is a pricing opportunity for the manufacturer that holds that secret. When there is no secret, but instead, an open environment, then the pricing will be based on the product cost. In the case of an application, the writing, distribution, and absorption of the public key data of the app will drive the cost model. For NFC cards, there is the cost of the JAVA chip card, which is widely used for many environments, and which has a very low cost. A simple PKOC card from a card manufacturer is less than $5.00 today. The cost for combination cards with multiple credential types will be priced more by the older symmetric credential types than for the PKOC credential in the card and you can find this on Amazon today starting at $10.00.

Simplicity
PKOC is simple compared to the symmetric card technologies that are the basis of most cards in today's market with multiple common bit format configurations available. In the access control system, in order that the information that comes from the reader to the access control panel is understood, the parameters of this format must be entered. This will include the length of the key and the breakout of the facility code versus the actual credential number. There are start and stop bits to consider. There is the ordering process for the cards where it is critical that the ordered cards do not duplicate any that are presently in the user's environment.

The card manufacturers have created systems and controls for the above issues, and the costs to support them are priced into the card cost. With PKOC, none of these controls are required.

PKOC Information
- In the case of a mobile device, the private key is stored in a TPM in the mobile device and never leaves the TPM (Trusted Privacy Module).
- In a Java card, the private key is stored in a TPM in the Java card and never leaves the TPM.
- Public Key Open Credential (PKOC) is a specification that provides a secure way of using asymmetric encryption with the public key portion as a credential. PKOC does not require a members, royalty, or special license to be utilized and is truly open for all that want to utilize the specification. In today's security industry, the openness of this is a

major differentiator, and it is also rare in that the industry largely relies on symmetric encryption for today's credentials. PKOC also does not come with all the complexity and infrastructure of the asymmetric options that do exist today such as PIV/CIV based credentials.

- PKOC, pronounced /ˈpēˌkäk/ (like peacock) is the acronym for Public Key Open Credential. PKOC represents an openly available specification, written and supported by the Secure Credential Interoperability (SCI) Working Group of the Physical Security Interoperability Alliance (PSIA) https://psialliance.org/. The specification defines a highly secure, access credential solution designed to enable interoperability. The specification is posted here (https://psialliance.org/securecredentials/) with the intention to make it readily available to end users, manufacturers, integrators, virtually anyone who wants to develop an app with a self-generating access credential in it or develop a device (reader or panel) that will consume the highly secure credential for physical or logical access needs. This highly secure credential option will put the control back into the hands of the security practitioners. Conforming to the IT Industry Standard for Public Key / Private Key pair generation, PKOC is agnostic to the transmission method, whether it be NFC, BLE, UWB or whatever new transmission technology exists down the road and is fully compatible with iOS and Android devices as well as Java chip access cards
- Currently, all wallet-based credential providers are issuing proprietary symmetric key pairs for their credentials which they generate and control (SeoS, LEAF, MIFARE, and Universal). A proprietary symmetric key must be shared with other manufacturers in a secure manner for the credential on the phone to be read. In most cases the originator of the symmetric key will either sell a module or a license to other manufacturers, which adds cost and ultimately results in dependence on a single manufacturer/vendor to expand the ecosystem. Aside from the inherent risks in the process of key sharing, this means the User of the credential is locked into that manufacturer and their partner choice, which may not necessarily align with your objectives. Even if they proclaim having an open policy, meaning they will share keys, the choice remains theirs, not yours and they may be capitalizing on your situation by charging more money, often on a recurring basis. At this point you are essentially locked into a single vendor! The PKOC credential is Asymmetric, therefore it is highly secure from the start because no one, not even you, has access to the private key; it remains on the secure element/TPM in the phone or chip card and is never shared. The public key may be shared amongst multiple systems and devices, without any security concerns. For this reason, it is extremely simple AND interoperable, with no strings attached. Any manufacturer you wish to work with may download the PKOC specification from PSIA at (https://psialliance.org/securecredentials/) and enable their devices to read that credential.

More about Question 3 - Who benefits from PKOC from a security perspective?

End User
It is the end user that is investing in security for their locations. Each controlled opening will have a significant cost to install. Access controlled doors are not inexpensive when done well. There are many ways to configure a door for a low budget, and each budget compromise in the installation increases the vulnerability of the opening.

The use of PKOC as the credential puts the attack surface at 1, not thousands or, in some cases, millions.

The concept of an attack surface has many parallels in basic physical security. Consider a fleet of armored vehicles that move cash between banks and businesses. There are multiple security elements on each vehicle that run from the physical nature of the tires to the staffing within the vehicle. Determining how to compromise one of these vehicles provides, at least for a short time, the plan on how to compromise many of these vehicles. And if that compromise is based on the manufacturer of the vehicle that is purchased by many different independent fleets, then the collaboration between these fleets is likely to be relatively weak. The fact that there are many of these vehicles defines the size of the attack surface. If the cost to the nefarious actors to come up with a successful attack for one vehicle is high, that cost may influence them to move on to other targets or other approaches. But if that high cost can be spread across many different fleets and vehicles, then the cost becomes more reasonable. It is the large size of this attack surface that makes the nefarious investment viable.

PKOC is based on x.509 elliptical curve key pairs. X.509 certificates are digital documents that represent a user, computer, service, or device.
https://csrc.nist.gov/glossary/term/x_509_public_key_certificate

As a technology, PKOC is a subset of CBA (Certificate Based Authentication). It is a subset because it simply uses the public key as the access credential. There is no Certificate Authority, as in PIV and CIV (Personal Identity Verification and Customer Identity Verification).

The specifications that are published by PSIA and are publicly available at no cost to anyone and any organization, manufacturer, or user community have defined that a minimum of 64bits and anything up to the 256 bits of the X portion of the public key is functional. A 64 bit number has a decimal equivalent of 18,446,744,073,709,600,000. A 128 bit number has a decimal equivalent of 340,282,366,920,938,000,000,000,000,000,000,000,000. These numbers represent the possible generation of unique certificates represented by the utilized bit length of the full public key.

Card technology has progressed from Hollerith (cards with holes in particular positions in the card), to Wiegand wire cards where Wiegand wires embedded in plastic cards, positioned so that they projected 1s and 0s when the card was swiped through a slot in a card reader, to PROX cards. There is almost zero use of Hollerith or Wiegand wire cards that remain today.

PROX cards are generally considered to be the start of RF smart cards. A 125KHz excitor field from a card reader will power the PROX chip which will then spit out a card number. There are no security elements in a PROX card.

Wiegand wire cards needed a way to communicate the card numbers and a communication format we created. This is the genesis of the Wiegand communication, a one-way card-to-panel data transmission.

Decades later, with card technology slowly progressing, the need for a greater amount of data to be transmitted and the need for bi-directional communication, the concept of OSDP (Open Supervised Device Protocol) has now become the next generation of reader communication. With OSDP Secure Channel, the communication is now bi-directional, electrically differential because it is based on IEEE RS485, and encrypted.

For all the decades of Wiegand communication usage, most readers were wired with 6 wires: +, -, D1, D0, LED, and Buzzer. While most marketed readers had some form of tamper switch, it was almost never employed. Firstly, it would have required one more wire. Secondly, it was often an open collector, not a dry contact, and that was not easy to connect to typical access control panels. In about 2020, multiple hacks were published on the internet that provided easy ways to compromise Wiegand communication. These hacks helped to slowly move the market toward OSDP.

When using PKOC, while it is possible to use a Wiegand communication PKOC reader, the market is almost entirely based on ODSP. The use of OSDP Secure Channel will enhance the overall security posture of the access control system.

Because of the use of Wiegand wires that were embedded in plastic cards that were positioned so that they projected 1s and 0s when the card was swiped through a slot in a card reader, the communication protocol that was used for that card reader communication was adopted by other technology cards and readers. The communication protocol that was created and named Wiegand communication format is the most widely used reader connection methodology.

Other communication protocols do exist including 20 milliamp current loop and basic RS485 that is custom to the systems that use this. However, OSDP (Open Supervised Device Protocol) has now become the next generation of reader communication.

If you are an integrator, you need to deal with the existing card/reader populations of your clients. Possibly they have 26bit Wiegand PROX at one site, iCLASS at another, SEOS at a third, and DESFire EV2 at a fourth. Assuming that there was no coordination of these when they were installed, possibly because they were acquired or just independently managed, you could see duplicate card numbers even across these different ecosystems.

Then there is the facility code and card number format that needs to be assigned in the access control system and put into each panel. With the older technologies, the card number fields were smaller and multiple facility codes needed to be used on single sites. Sometimes these settings are not straightforward. And ordering the next set of access cards can be a challenge if the end user did not end up with a management methodology, at a cost, with something like HID's Corporate 1000 system.

When using PKOC, while it is possible to use a Wiegand communication PKOC reader, the market is almost entirely based on ODSP. The use of OSDP Secure Channel will enhance the overall security posture of the access control system. Since the readers will need to be replaced to use PKOC, moving to OSDP at the time of new reader installation will enhance security.

More about Question 4 - Who benefits from PKOC from an interoperability perspective?

In multi-tenant buildings today, when the building uses access control on their garage, their main entry doors, possibly lobby turnstiles, and possibly elevators with cab readers or with destination dispatch systems, these systems are unlikely to be the same as the building tenants would use at their sites. If the tenant just utilizes whatever their landlords use, those that travel between sites will end up with many access cards. If the tenant spaces are standardized across their properties, then it is likely that their employees will be carrying two cards, one for the building and one for the organization. While there are workarounds for these situations, they are always challenging and add cost and complexity.

A landlord is an end user, just as a tenant is. If they were both to adopt PKOC, then the challenges with card types, bit length, facility codes, and card numbers would go away. PKOC is open and all systems can utilize PKOC without any restrictions or license fees. Certainly, there are transitions here that will take time to resolve. But building owners and elevator companies are interested in the longer term potential of this open infrastructure.

In the US market, the most common types of more secure card technologies are the HID Seos and NXP DESFire EV3. Considering each of just these two types of credentials, there are interoperability considerations.

HID Seos

- All Seos products are ultimately sourced through HID.
- Seos cards can contain multiple Secure Identity Objects (SIOs), each of which is a credential. Therefore, it is the SIO that is important here.
- HID has generic Seos cards with a generic SIO symmetric key, those that can be purchased through multiple channels including general security distribution.
- All generic Seos cards contain the same symmetric key and that same key is also in all generic Seos readers.
- When a third party manufacturer makes a contract with HID to be able to be able to read Seos cards in their product, they purchase a small electronics part, like a mobile phone's SIM card, to put in their reader. That SIM has the symmetric key.
- The cyber-attack surface for this symmetric key is the sum of all the cards and all the readers that have been produced.
- Elite is HID's program where they will create a symmetrical key that "belongs" to the Elite customer. Any enterprise can become an Elite customer with a symmetric key that is in all their cards and readers.
- The attack surface for an Elite symmetric key is the sum of all the cards and all the readers that have been produced for this customer.
- The Elite key lowers the attack surface dramatically.

HID reported a vulnerability in February 2024 that allows attackers to read credential and device administration keys from configuration cards, potentially creating malicious cards or credentials. This affects HID iCLASS SE CP1000 encoders and related products. The vulnerability arises from certain configurations in the communication channel for encoders, exposing sensitive data. HID recommends moving from "generic SEOS" to Elite to enhance security and mitigate downgrade attacks. Please contact HID or see the following article for more information: https://www.securityinfowatch.com/access-identity/article/53095490/hid-divulges-vulnerabilities-to-its-iclass-se-cp1000-encoder

NXP DESFire EV3

- The EV3 cards can be purchased through any source that purchases NXP products. There is a wide range of organizations that can provide EV3 cards.
- NXP provides a framework for protecting the chip, the ability to add applications, and the ability to create the symmetric keys for each level and for the credentials themselves.
- Many organizations have moved to NXP so that they can control and “own” the keys.
- Another framework was defined and fully published by WaveLynx called “Leaf”. That framework defines a structure that utilizes the opportunities that NXP provides in their chips and tries to solve the interoperability challenges that ensue from NXP’s “free-for-all” opportunities. The Leaf concept was a valiant attempt to put some structure for EV2 and EV3 NXP access control, but this has not taken hold and is almost solely utilized by users of WaveLynx readers.
- Where an organization utilizes their own set of symmetric keys with EV3, the attack surface is the sum of all the cards and all the readers that have been produced for this customer.

More about Question 5 - Who benefits from PKOC from a cost perspective?

End User

The end user ultimately benefits with PKOC from a market that is less complicated and free from proprietary product offerings.

- The open and publicly available specification for PKOC allows any entity to enter this market. There are no restrictions, and no licensing fees, royalties, or memberships required for proprietary products.
- The process to set up the access control system to accommodate the format of PKOC is simply one of defining the bit length between the minimum 64-bit up to the full 256-bit credential key in the access database.
    - Due to the long history of smaller credentials, like 26bit, 48bit, and many others in between, access control system enrollment screens are not necessarily formatted to make this entry directly.
    - But most access systems of any significant market presence do have ways of supporting PIV cards which are 200bit.
    - There are wedge readers for ease of enrollment of PKOC credentials.

Integrator

As the PKOC market matures, more individuals that set up and program access control systems will find that PKOC is less complicated.

- The integrators and installers benefit from reduced complexity and faster installation time enabling more jobs and revenue opportunities.
- Training expenses will be lower.
- For the symmetric keys today, determining the right bit length, facility code, and card number formats, and setting them to be usable in the head end and panels can be challenging.
    - This effort is often hard to effectively monetize.
- A PKOC card is simply that. It comes in one format. When asked by a reader to communicate, it provides its full public key.
    - The reader decides (and must be set) so that it sends on the credential as the bit length that is set in both the reader and the access control panel. There is no difference in the PKOC card and no difference in the public key that it sends.
    - If an end user's system is set to utilize a credential of 128bit but a landlord's system is set to utilize a 64bit credential, the same PKOC card supports both.

Manufacturer

The manufacturer benefits from PKOC by reducing the format complexity and compatibility matrix for testing that lowers their overall manufacturing costs and improve profit margins.

- It often comes down to the manufacturer's support people to help integrators, end users, and consultants resolve symmetric credential setup issues and problems.

Consultants

Consultants support end users with more than just physical system designs. There are all the other complexities that come up where the end user has a challenge and needs a translator and support person.

- Cards
- Readers
- Card or reader ordering
- Forms that are confusing for end users to fill out but required to manage the distribution and availability of secret symmetric keys.
- Management of credential numbers within symmetric key systems

Consultants are not always in a good position to monetize these perioral activities.

More about Question 6 - How does PKOC work?

The card manufacturer can provide cards that have PKOC ready to use. An integrator could purchase JAVA cards and program them, but they would need to write the JAVA code to the PSIA specifications. An end user could also program the cards. But why would an integrator or end user spend the time and effort to do this programming when there is no security secret that would be exposed. The outcome would not be different. The private key is safely stored in the processor with the OS that had a KeyGEN command available.

Background on Public Key cryptography
There are two processes, both of which obscure the actual data, that are used for two very different purposes. One is *SIGNING* and the other is *ENCRYPTING*.

SIGNING provides assurance that the message is coming from the person that it says it is, Person A, very much like signing a name to a letter. The reader can see the signature and recognize that it is truly from person A. *SIGNING* uses the private key to sign the data. When the receiver, person B, uses the other half of the key pair, person A's public key, to validate that the data actually came from the source that it expected, person A, the message returns to a readable form.

ENCRYPTING uses a public key of another party, person B, the receiving party, to encrypt the data so that others cannot decode the message. If party A shared their public key with person B, and person B shared their public key with person A, then it is possible to effectively hide the message twice by *ENCRYPTING* and *SIGNING* a message. This will ensure that the message is not readable by anyone but the receiver and that it came from the sender and no other source.

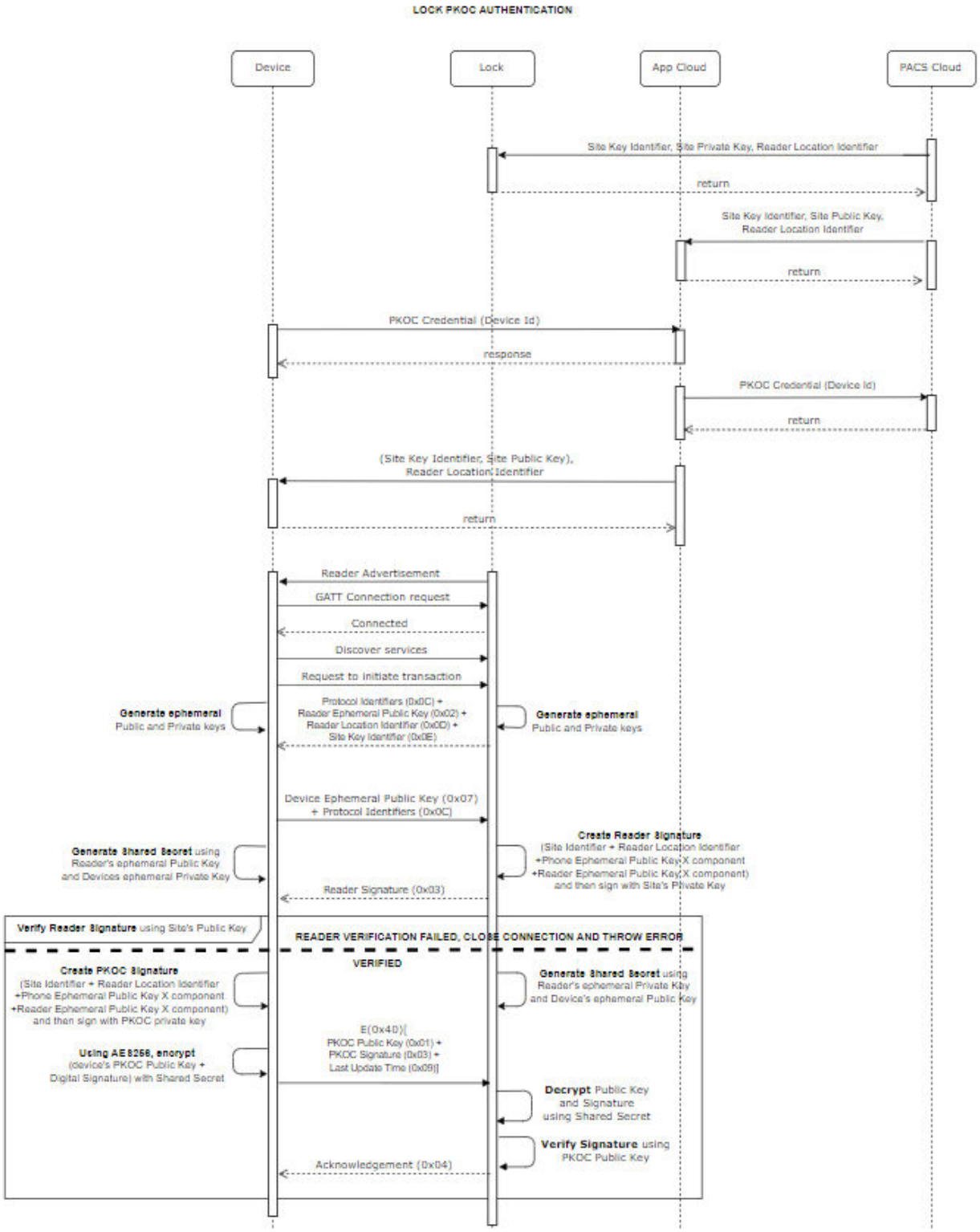
For the purposes of PKOC, the *SIGNING* operation is the one that is used to prove that the card or mobile device that has the private key in a protected vault is the one that is sending the signed message. No credential imposter, such as a cloned card, or some electronic device that is attempting to pretend to be the credential, will have had access to the private key. When the card reader attempts to review the one-time message that it sent to the reader using the credential's public key, it will not come back as equaling the same message and will not be accepted.

The PKOC Card and Reader Transaction Process
When a card is presented to a reader, the steps of the process are described below and a flow diagram is on the page that follows this description. All the statements are based on a card being presented, but the general flow is the same for a Bluetooth mobile device is used.

- The reader sees a card being presented.
- The reader sends out a SELECT command.
- The card receives the SELECT command and formats a SELECT RESPONSE.
  - The card formats a message with the card type and a success response
- The card sends the SELECT RESPONSE.

- The reader receives the SELECT RESPONSE.
- The reader creates a TRANSACTION ID that is based on the correct protocol.
- The reader sends an AUTHENTICATE COMMAND, inclusive of the TRANSACTION ID.
  - Authentication command + Protocol Version + Transaction Identifier + Reader Identifier.
- The card receives the AUTHENTICATE COMMAND and creates the AUTHENTICATE RESPONSE.
- The card sends the AUTHENTICATE RESPONSE.
  - This message includes the 65Byte public key + the 64Byte signature and the *SIGNED* response code.
- The reader receives the AUTHENTICATE RESPONSE.
- The reader validates the AUTHENTICATE RESPONSE.
  - The reader uses the card's full public key to *DECRYPT* the *SIGNED* AUTHENTICATE RESPONSE using standard processes.
  - The reader compares the TRANSACTION ID to the decrypted TRANSACTION ID.
  - If the result of the decoding gets back the AUTHENTICATE COMMAND that was sent to the card, that means that the card has not been cloned and is valid.
- The reader sends the credential over OSDP to the access control panel.
  - This could also be Wiegand, but OSDP is preferable and more flexible.
  - The credential is a portion of the public key that is set in the reader and the access control panel.

The public key is actually 65Bytes (520bits). With Elliptic Curve Cryptography (ECC), which is used for PKOC, all or a portion of the X information within the 65Bytes can be used as the credential. That is why the statement above indicates a "portion of the public key" (where all the entropy exists). It is up to the reader and panel settings to determine how many bits of the X portion of the key to use starting at a minimum of 64bits up to the full 256bits of that portion. The specification recommends a minimum of 64bits and anything larger than that is better. The use of the full X portion of the key (256bits) has been demonstrated. 128bits is a reasonable size for most ACS manufactures since it is within the PIV specifications. 128bits provides very high security.


LOCK PKOC AUTHENTICATION
Device
Lock
App Cloud
PACS Cloud
Site Key Identifier, Site Private Key, Reader Location Identifier
return
Site Key Identifier, Site Public Key, Reader Location Identifier
return
PKOC Credential (Device Id)
response
PKOC Credential (Device Id)
return
(Site Key Identifier, Site Public Key), Reader Location Identifier
return
Reader Advertisement
GATT Connection request
Connected
Discover services
Request to initiate transaction
Generate ephemeral Public and Private keys
Protocol Identifiers (0x0C) + Reader Ephemeral Public Key (0x02) + Reader Location Identifier (0x0D) + Site Key Identifier (0x0E)
Generate ephemeral Public and Private keys
Device Ephemeral Public Key (0x07) + Protocol Identifiers (0x0C)
Generate Shared Secret using Reader's ephemeral Public Key and Devices ephemeral Private Key
Create Reader Signature (Site Identifier + Reader Location Identifier +Phone Ephemeral Public Key X component +Reader Ephemeral Public Key X component) and then sign with Site's Private Key
Reader Signature (0x03)
Verify Reader Signature using Site's Public Key
READER VERIFICATION FAILED, CLOSE CONNECTION AND THROW ERROR
VERIFIED
Create PKOC Signature (Site Identifier + Reader Location Identifier +Phone Ephemeral Public Key X component +Reader Ephemeral Public Key X component) and then sign with PKOC private key
Generate Shared Secret using Reader's ephemeral Private Key and Device's ephemeral Public Key
Using AES256, encrypt (device's PKOC Public Key + Digital Signature) with Shared Secret
E(0x40)[PKOC Public Key (0x01) + PKOC Signature (0x03) + Last Update Time (0x09)]
Decrypt Public Key and Signature using Shared Secret
Verify Signature using PKOC Public Key
Acknowledgement (0x04)

More about Question 7 - Why is there no need for a centralized key management system?

Revocation.
PKOC does not have a centralized management system and therefore, does not envision or use the concept of revocation across all uses of the credential. Is this important to the security of the utilization of PKOC?

PKOC is a very secure, simple way to create and use an immutable credential. These credentials cannot be cloned, and they cannot be changed or adapted. Most in the security technology industry have heard of “KeyMe kiosks and “Flipper Zero”. These two are used to compromise older card technologies. Note that history shows us that all symmetric key approaches are vulnerable to compromise.

Revocation of a card, as in the approach that PIV uses, has a purpose and value. The concept of PIV was and is that a single PIV card can be used at different government entities. That multiple entity concept hasn’t been very effective, with many people running around with multiple PIV cards for different entities. Organizations take the permissions of access credentials out by making a change to their access control systems via any of multiple approaches. There is little need today to change multiple access control systems on-mass. Decades ago, access control systems were often of the same brand but independent at different sites. Today, most multi-site access control systems are either one larger system or there is a PSIM (Physical Security Information Management) system that integrates with each of the independent systems.

None of the presently available symmetric credentials could support a revocation process.

More about Question 10 - What to specify for a PKOC system?

Given that the PSIA specifications define the entire process with all the technical information required for success and given that the security industry has a penchant for "privatizing" technology, it will be important for those that are specifying systems and PKOC usage to help maintain the "open" nature of PKOC.

Any member in the supply chain might want to privatize their PKOC process, thus killing any opportunity of taking advantage of the OPEN nature of PKOC. To do this would be quite simple. The PKOC specification has an Application Identifier (AID). All PKOC cards and readers use this same AID. The PSIA specified AID is "A000000898000001" If a card or a reader were to use a different AID, then the reader or card that is being used in a system would not match and the process would stop at that point. Why might this happen?

- Manufacturers might want to create their own set of PKOC cards and readers so that they could become the sole source of these products for a client, thus allowing them to sell products at a higher price, since they would not be an open market item. This is common with symmetric keys.
- Integrators would have the same reasons for privatizing the AID, and some in the marketplace might think that it would make sense for a large integrator.
- The two cases above would break the open characteristics of PKOC, limit the supply chain, and ultimately add cost to the end user.
- End User organizations might want to "have their own cards and readers."
    - In this case, the organization would be hurting themselves in that they would not be able to take advantage of the open nature of PKOC. An example of the problem with this is where that organization has a sales office in a multi-tenant building that has PKOC readers available. They would not be usable.
    - The restriction created by requiring a different AID would likely tie the organization to a single supplier and higher prices would result.
    - There would be no security advantage to the end user to have a "private" AID.

Having your own key for an organization, when using symmetric keys, makes great sense. It limits the attack surface, thus providing a lower perpetration value and likelihood that a hacker would invest in trying to hack the organization's card and reader system. But having your own AID with PKOC would just tie the organization to higher prices, limited supply chain opportunities, and delays in supply of products.

When purchasing a wedge reader, it will be important to specify the type of system and the bit length so that the wedge reader can fill in the right data into the credential field. Remember that the bit length that comes out of a card read is 64Bytes or 520bits. The specification recommends anywhere from 64bits to 256bits. 128bit credentials are commonly used and very secure.

- This device requires that you specify
    - The bit length that you want to use for the ACS

    - The brand of ACS
        - For some ACSs, it is important to put the curser in the right spot on the enrollment screen and to have a wedge reader that will put the portion of credential in that first spot, automatically tab one or more times to the next field, enter that data, tab to the next field, and finish the last of the credential.
- It is a reasonable potential that a PKOC supported reader for a multi-tenant building will have a different bit length than that which is used for an organization's internal use. The landlord for the multi-tenant would then need to have a wedge reader that is configured to work with the landlord's system that would be configured differently from the organization's reader.

Tools that are available to a consultant to use in a PKOC design:

- The specifications on the (https://psialliance.org/securecredentials/) for NFC and BLE
- IDmachines Eidola device for OSDP tracing
    - This can be purchased from IDmachines through Salvatore D'Agostino (sal@idmachines.com).
    - MSRP for the total kit including the base and tools including PKOC is $2,593.50
    - Further details are at IDmachines – Security without compromise
- The PKOC Test Board (reader)
    - Attached below are two guides on how to interface with the Last Lock PKOC Dongle. It should be plug-n-play. The first document breaks down how to interface with the dongle without a development kit, the way you have it. The second document talks about developing and running custom code on the Dongle using a nRF52840-DK.First, plugging it in should make the advertising LED light up and you should be able to scan and connect to it using the PKOC Service UUID. Sending a nonce request should send you a nonce with the Source GUID and you should be able to do the PKOC Normal Flow. Additionally, included a number of slides from the PSIA Technical Resources Review including github links and reference material.
    - It is recommended that you consider participation in the PSIA PKOC working group through membership with PSIA for support resources, but this is NOT REQUIRED.

- Mobile App and Android Reader Simulator source code from JCI
    - You can e-mail glenn.holton@jci.com and he will send a software use agreement to acknowledge. Once that is completed, he can provide a link with all the source code for mobile apps on Apple, Android and a reader simulator on Android.

More about Question 11 - How should a consultant design and specify PKOC?

Consideration as to the approach to enrolling a PKOC card in an access control system (ACS) must be given. Typically, the enrollment screens were designed to easily support around 50bits. But that doesn't mean that the systems can't support additional bit sizes, especially if the ACS supports PIV card size bit formats.

There is a process that needs to be understood and implemented. Once that process is clear and tested, a wedge reader can be procured that can be set up to automate the enrollment entry process. As of October 2024, SBD has only tested this wedge reader enrollment process on JCI's CCure9000 and that process requires the wedge reader to split a 128bit credential read into three pieces and use multiple tabs in the output to make the wedge reader work well with a single card presentation to the wedge reader at a specific place on the enrollment screen. The setups for other systems will likely be similarly convoluted. Once resolved, the rest of the process is straightforward.

Jason Ouellette has tested a full 256bit public key on the CCure9000 as well.

PSIA has published a third specification that is an extension of OSDP that defines how to move the data through the reader and do the PKI work in the access control panel instead of at the reader. This process has been demonstrated in lab conditions but is not available at the time of distribution of this document.

- The specification is available at https://psialliance.org/securecredentials/)
- **PKOC over OSDP Specification 1.63- Approved Mar 22, 2024**

More about Question 12 - When and how would PKOC be available as a wallet product?

Currently, all wallet-based credential providers are issuing proprietary symmetric key pairs for their credentials which they generate and control. A proprietary symmetric key must be shared with other manufacturers in a secure manner for the credential on the phone to be read. In most cases the originator of the key pair will either sell a module or a license to other manufacturers, which adds cost and ultimately results in dependence on a single manufacturer/vendor to expand the ecosystem.

Aside from the inherent risks in the process of key sharing, this means the User of the credential is locked into that manufacturer and their partner choices, which may not necessarily align with your objectives. Even if they proclaim to have an open policy, meaning they will share keys, the choice remains theirs, not yours, and they may be capitalizing on your situation by charging more money, often on a recurring basis. At this point you are essentially locked into a single vendor!

The PKOC credential is Asymmetric, therefore is highly secure from the start because no one, (not even you) has access to the private key. It remains on the secure element in the phone or chip card and is never shared. The public key may be shared amongst multiple systems and devices, without any security concerns. For this reason, it is extremely simple AND interoperable, no strings attached. Any manufacturer you wish to work with may download the PKOC specification from PSIA (https://psialliance.org/securecredentials/) and enable their devices to read that credential.

More about Question 13 – How should a consultant plan to migrate an existing card environment to PKOC?

When looking at all that needs to happen to migrate a system from a symmetric key system to a PKCO asymmetric key system, it just seems pragmatic to do a full rebadging first and then change out the readers when capital projects can fund the change. Priorities for areas or programs can be set.

It is recommended that a migration card be used to move from one or more present credential technologies to a straight PKOC system. Migration cards would have the new PKOC credential and the old symmetric credential in them and available to be used. There might be a value in additional credentials to be in the cards as well.

Many of the “hacks” that have been shown on asymmetric card technologies have included the transformation of the information in the card from one technology that appeared secure down to an older and less secure technology that the card reader can also accept. In some cases, those technologies have been turned off at the readers, but only to be turned on again by part of the hack using program cards. In other cases, all the older technologies were just supplied and left unmanaged in the reader for the convenience of the integrator, consultant, or system administrator.

Once the user community has been re-badged, or when all card holders have a new credential, then a reader that has only PKOC capability will limit what can be done at the door.

From the panel side, with just the planned bit length of the PKOC read entered into the ACS panel, the system should be secure in terms of credentials and readers.

From the reader to panel communication perspective, when using OSDP Secure Channel, the data transfer between the readers and the panels should be secure.

PKOC Development Kit

Description:

In order to increase ease of access to PKOC compatible hardware and firmware, the design and manufacturing of a universal development kit has been approved by PSIA. The dev kit will allow all PSIA members to program and test firmware implementing PKOC over BLE and NFC in a Nordic environment. In an effort to increase reliability and decrease cost, an existing nordic dev. board will be used as the foundation of the kit. While the NRF52840-DK ($49) is an ideal candidate with both BLE + NFC capabilities, the large form factor and high cost makes it a secondary choice to the NRF52840-DONGLE ($10) with a custom NFC daughterboard (DB). The DB will be designed to closely resemble the NFC schematic and BOM of the NRF52840-DK in a smaller package.

Requirements:

1. Design NFC DB to NRF52840-DONGLE that:
    a. Resembles size and shape of dongle board
    (example DB board size + aconno Antenna)

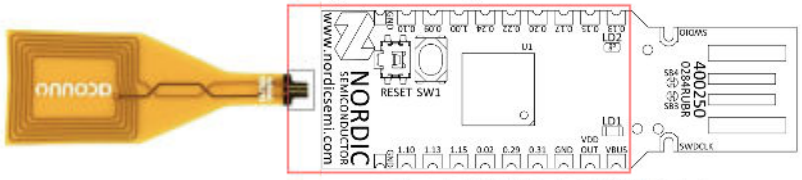


Figure 3: nRF52840 Dongle (PCA10059) front view

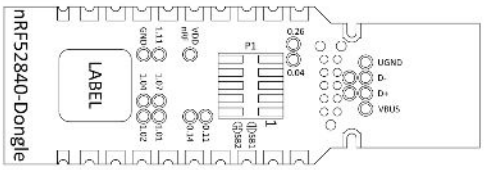


Figure 4: nRF52840 Dongle (PCA10059) back view

    b. Closely resembles the schematic and BOM of NRF52840-DK

Pins **L24** and **J24** are by default configured to use the *NFC* antenna, but if they are needed as normal GPIOs, **R44** and **R46** must be NC and **R43** and **R45** must be shorted by **0R**.

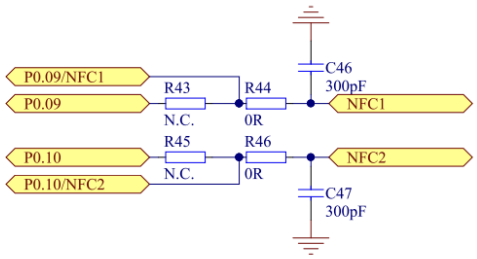


Figure 29: NFC input

    c. Uses premade + tuned NCF Antenna
        i. Possible option:
            1. Antenna: Aconno NFC Datasheet
            2. Connector: Molex 51281-0594

    d. Target price point of less than $20 per PKOC Dev Kit

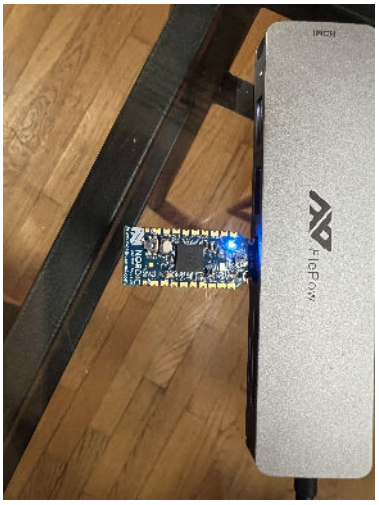
Working with the Last Lock Dongle

Initial Connection

Connecting the dongle to a USB port, should make it light up.

- On start up: Light blue
  - 

- Connected: Red
  - 
- Unlocked: Green
  - 
- Disconnected: Dark Blue

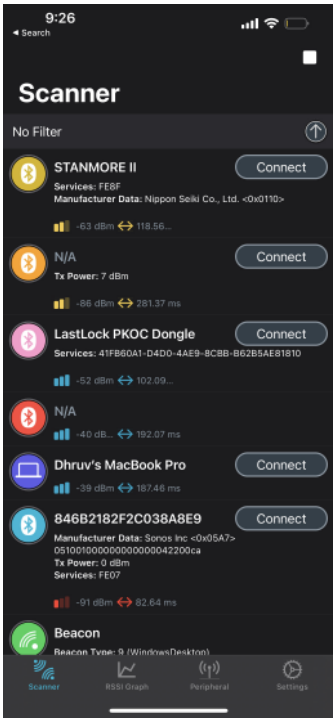
- 

Testing connections using nRF Connect:

Installing nRF Connect:

- Download the nRF Connect app from the IOS (apple store) or Android (google play store)

Connecting using the nRF Connect app:

- Open the nRF Connect app
- From the list of devices available select the "Last Lock PKOC Dongle"
  - 

- Connect to the LastLock PKOC Dongle:
  - If initial connection:
    - The light will change from light blue to red.
  - If connected before:
    - The light will change from dark blue to red.

- You should be able to see the PKOC Service and Read and Write characteristics and write random hex digits to validate functionality.

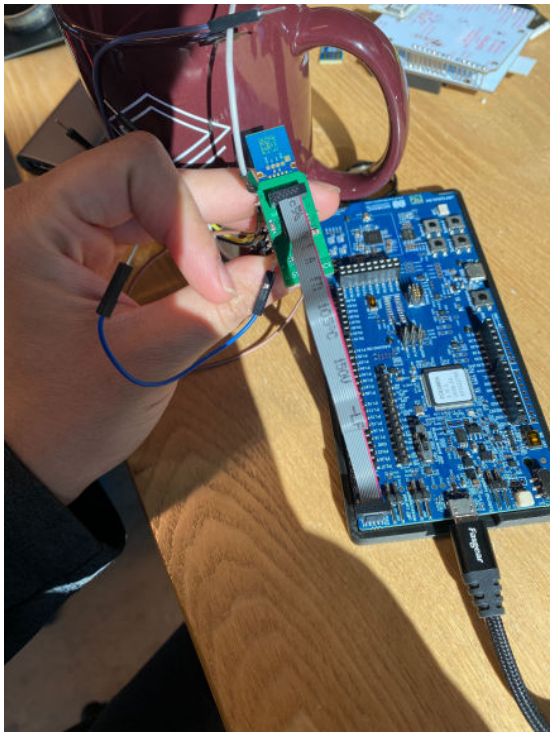
You should then be able to use your PKOC application or any of the other vendor PKOC applications to validate functionality.

Debugging Output from NRF 52840-dongle:
In order to get debugging output from the nRF52840 Dongle, you will require either an external J-Link or an nRF52840-DK.

- Requirements:
  - NRF-52840-dongle
  - NRF-52840dk
  - JTAG 2x7 Ribbon Cable

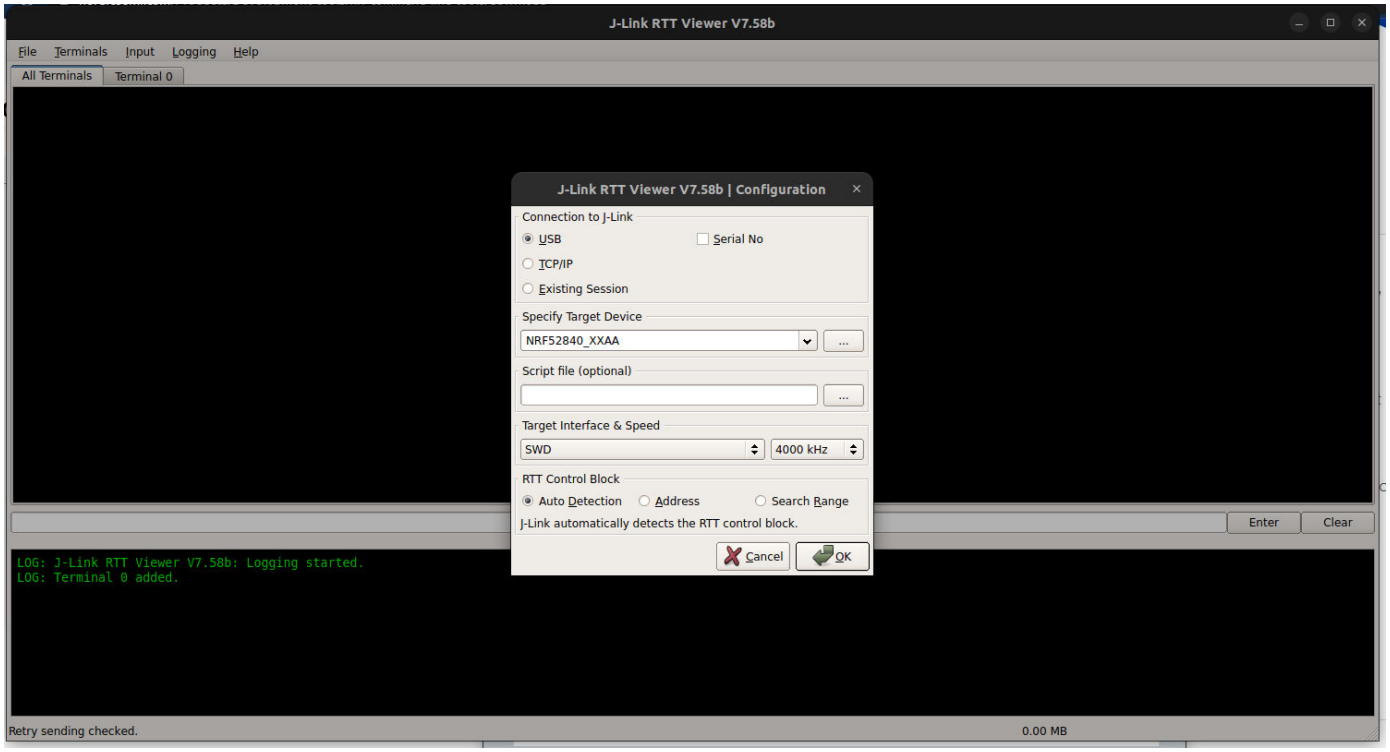
Instructions

- Connect the nRF52840 dongle and nRF52840 Dekit using the JTAG Ribbon Cable



- Install JLink Tools and Nordic Command line tools:

  nRF Command Line tools: https://www.nordicsemi.com/Products/Development-tools/nrf-command-line-tools/download
- Open up JLinkRTTViewer and Connect to the board using default settings.



- You should be able to connect successfully and see basic BLE Ouput from the firmware on the Dongle.

Developing with Last Lock nRF52840-dongle

Initial Setup:

Plug and Play:

- The dongle should be ready to plug into any USB Type-A socket and perform the appropriate tasks.
- If the dongle is not present then use the following guide on how to flash a hex file to the dongle

Getting Started

Requirements:

- JLink EDU/J-Link Programmer
- nRF Connect for Desktop
- nRF 52840-dongle
- A thunderbolt to USB type A convert to connect the nRF 52840-dongle
- Hex File to flash

Installing JLink

- Installation link:

> SEGGER - The Embedded Experts - Downloads - J-Link / J-Trace
>
> Download the latest SEGGER trial versions, eval packages and user manuals!
>
> https://www.segger.com/downloads/jlink/

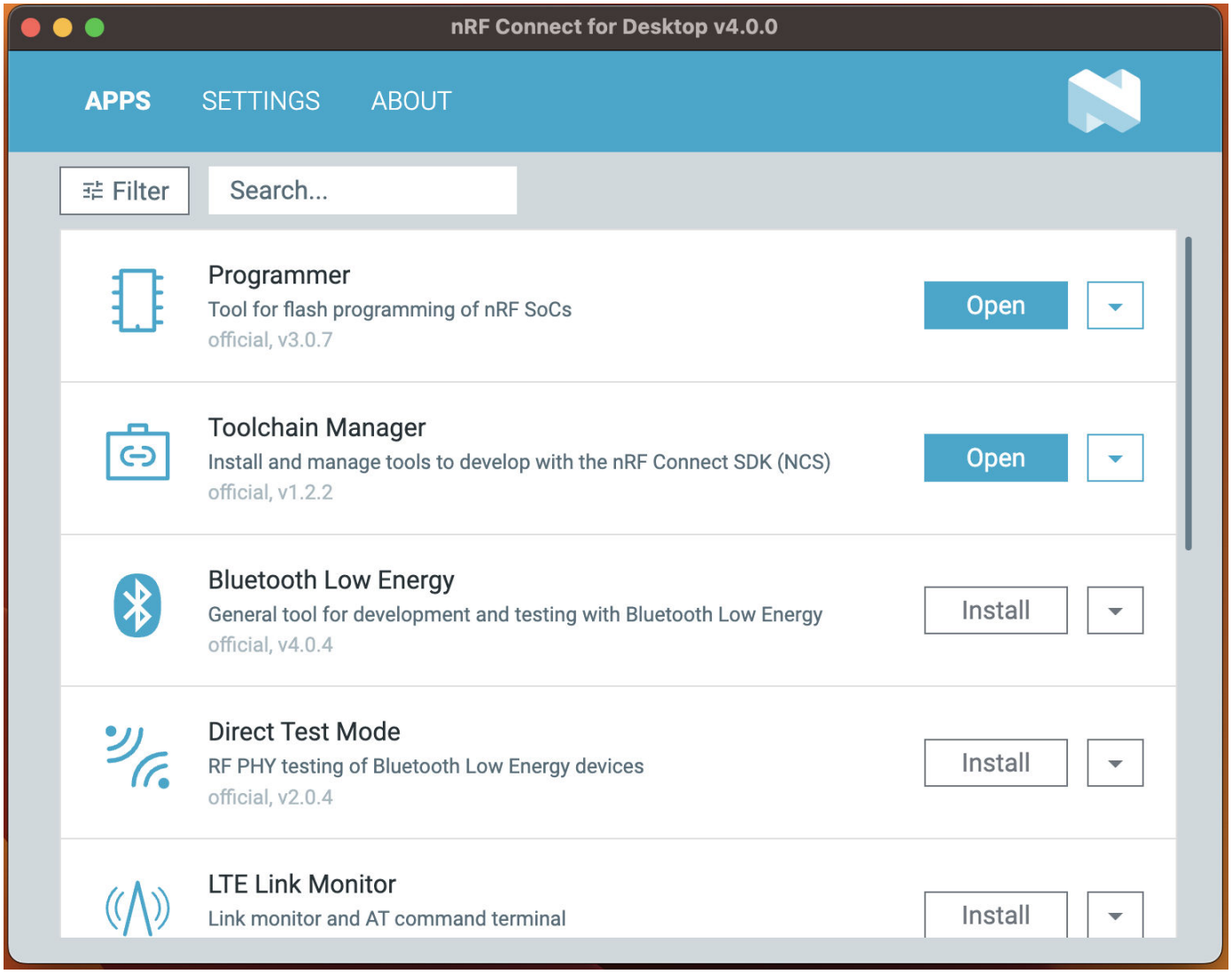
Installing nRF Connect for desktop:

- Installation link:

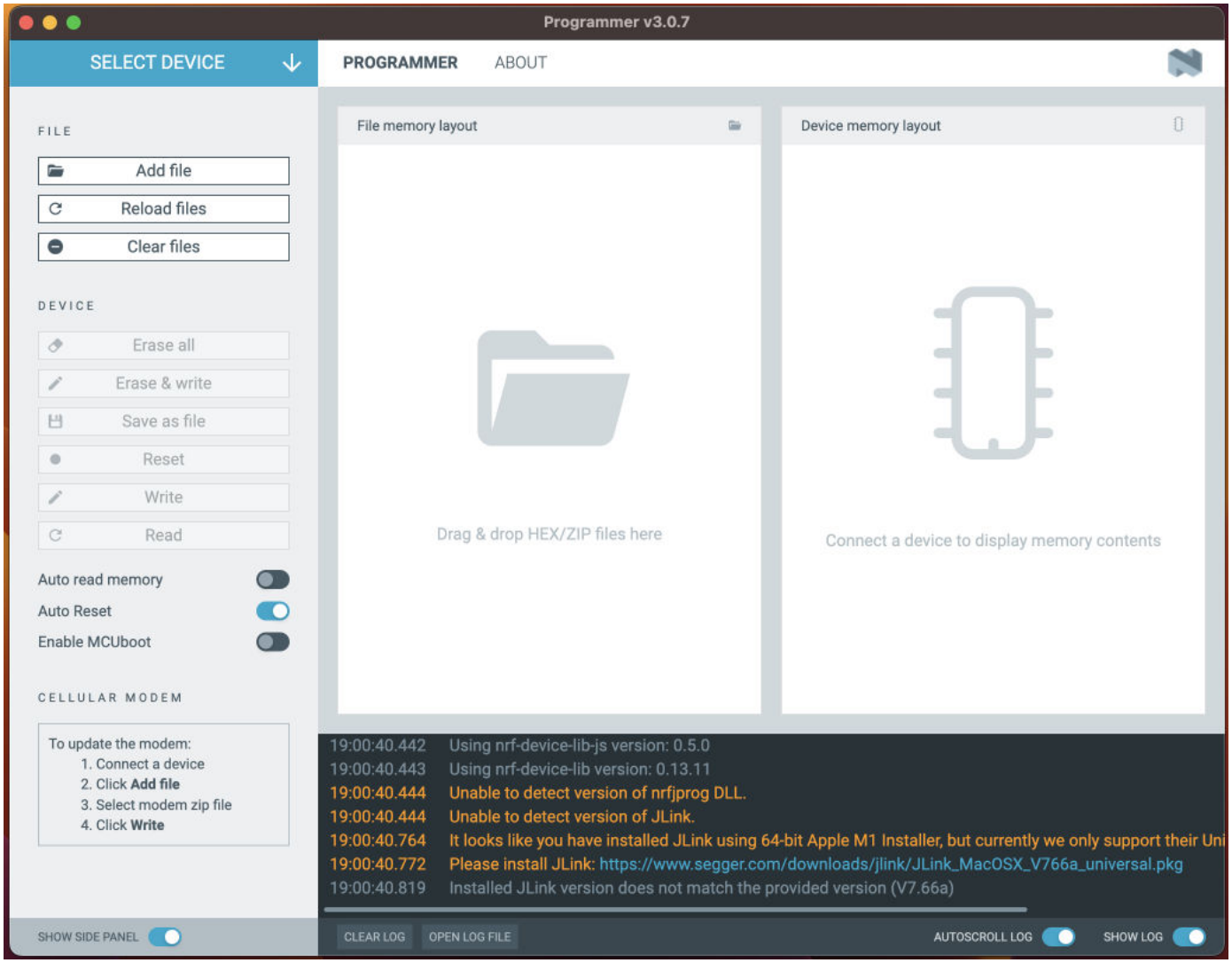
> nRF Connect for Desktop - Downloads
>
> Nordic Semiconductor
>
> https://www.nordicsemi.com/Products/Development-tools/nrf-connect-for-desktop/download

- Install the required version for the operating system that you are working on.

- Once installed nRF Connect for Desktop install the programmer application:



- Open the programmer. It will look like this:



Flashing a Dongle:

- Link on how to flash code to the dongle

> nRF52840 Dongle Programming Tutorial
>
> This tutorial demonstrates how to adapt and program SDK example applications to the nRF52840 dongle using USB DFU. It also describes how …
>
> https://devzone.nordicsemi.com/guides/short-range-guides/b/getting-star…

- Connect the NRF 52840-dongle to the computer.
- Put the dongle into boot-loader mode by pressing the reset button and seeing if the red LED blinks.
- Choose the device from the select device menu.
- Add the HEX file using the add file button
- If both are successfully added the write button should light up
- Write the code to the NRF 52840-dongle

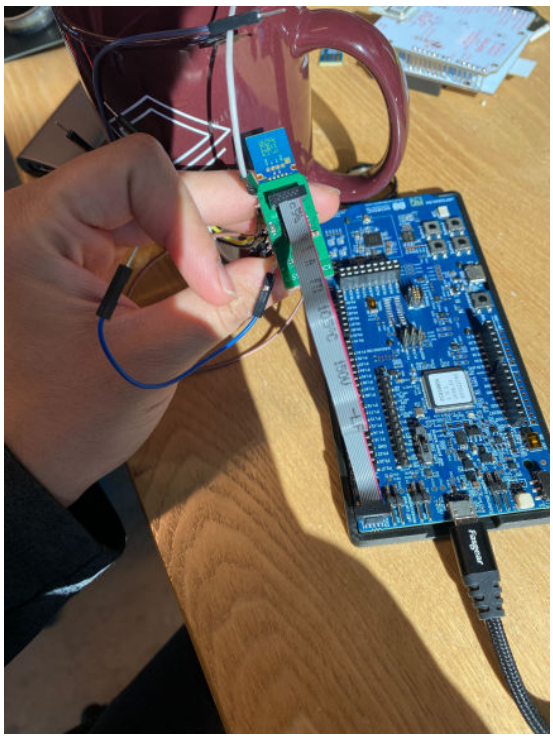
Debugging Output from NRF 52840-dongle:

In order to get debugging output from the nRF52840 Dongle, you will require either an external J-Link or an nRF52840-DK.

- Requirements:
  - NRF-52840-dongle
  - NRF-52840dk
  - JTAG 2x7 Ribbon Cable

Instructions

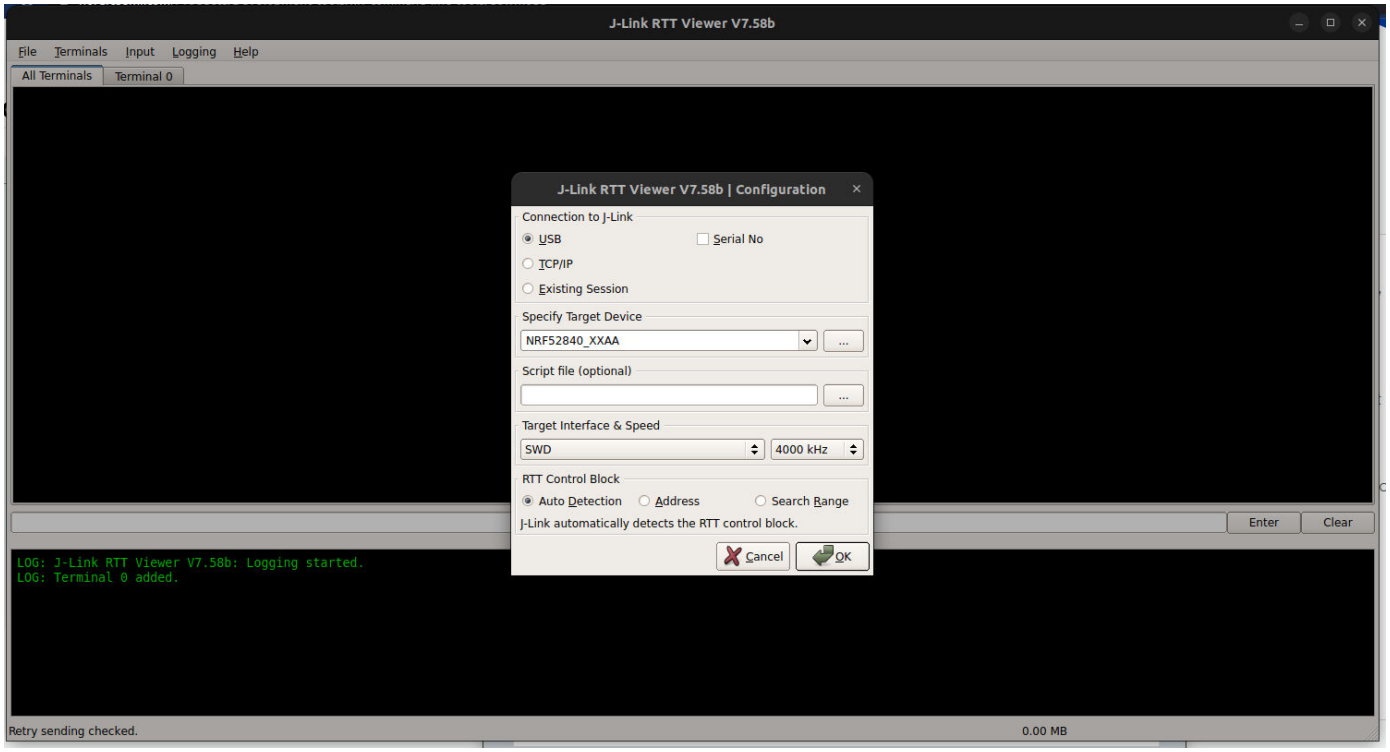
- Connect the nRF52840 dongle and nRF52840 Dekit using the JTAG Ribbon Cable



- Install JLink Tools and Nordic Command line tools:

  nRF Command Line tools: https://www.nordicsemi.com/Products/Development-tools/nrf-command-line-tools/download

- Open up JLinkRTTViewer and Connect to the board using default settings.



- You should be able to connect successfully and see basic BLE Ouput from the firmware on the Dongle.