Physical Security Interoperability Alliance

PKOC White Paper

Secure Credential Working Group

Laurie Aaron

9-5-2023

PKOC: Elevating the Experience of Secure Credentials

What is PKOC?

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 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 Infrastructure (PKI), 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.

How Secure is it?

The PKOC specification leverages the concept of PKI without the need for the typical complex, expensive identity Infrastructure necessary for PKI**. PKOC uses the device itself to generate the private & public key pair**, (known as keygen) enabling the private-public key handshake to authenticate the credential. The beauty of PKOC is that the private key never leaves the device and is born and stored in a secure element on the device (meaning if anyone were to tear the app/device apart, they could not get at the private encryption key), and the public key becomes the "badge #" which can be freely shared with any system or device used to control access. With a PKOC credential, the USER (owner of the phone or card) literally "owns" the encryption keys and does not require any complicated and often proprietary process for managing or sharing keys, as is the case with symmetric key solutions. The public key sharing process is straightforward without the cumbersome overhead of traditional symmetric key sharing processes, therefore Users no longer have to be burdened or distracted with the complexity of managing encryption keys. Furthermore, PKOC enables you to "Bring Your Own Credential" (BYOC) meaning a credential that is formulated in one app will work on all PKOC-enabled reader devices. There is no need to download multiple apps or carry multiple cards.

FUN FACT: ***Both Apple & Android mobile phones have had keygen capabilities since 2015.***

Why is there growing demand for Apple or Google Wallet access credentials?

Reason #1: Access credentials must be secure, the Apple & Google Wallet is an app that is locked down and secured by the device manufacturers (Apple and all Android device manufacturers), because it was originally intended for financial credentials. Because Apple limits the users of the Wallet, it ensures any app pushing a credential to the wallet is fully vetted and has passed the scrutiny of their security requirements. The Wallet apps are the only apps enabled to use Near Field Communications (NFC) on Apple phones to transmit data, Android has allowed any app developer to use NFC.

FACT: If you use a private-public key methodology such as PKOC, encryption keys originate in a secure element in YOUR device and private keys remain private and secure within your phone or card. The digital wallet becomes a moot point from a security perspective, albeit other conveniences.

Reason #2: The industry is accustomed to the credential feel of NFC technology; extremely reliable, but very short read distance (most smart and standard proximity cards use NFC). BLE offers a much longer read distance, however it is not as stable and reliable, while Ultra-Wide Band (UWB) is very reliable and supports long distance, it has not been widely adopted yet.

FACT: There are benefits to using access credentials in the digital wallet and other benefits to using BLE and UWB, which are addressed in the Credentials Comparison Chart matrix on the next page.

Reason #3: Apple has enabled the "Wallet" applications to be accessible even when your cellular phone battery is exhausted, therefore you may use your access credential even if your battery forces your phone to shut down.

FACT: While this is a valid reason for wanting "a wallet-stored access credential", one must weigh the risk and likelihood of phone exhaustion against the excessive cost of the currently offered Wallet credential infrastructure. In our research we have seen a range of $10-$30 per mobile access credential **per year to the end user.** It's noteworthy to point out that all wallet access credentials are not interoperable with one another, which leads to the need for multiple credentials in the digital Wallet to ensure interoperability. Today, multiple Wallet credentials will lead to excessive cost.

Reason #4. Apple and Google wallets leverage the users account as their "identity" which is widely accepted for accessing many online resources today. The Wallet then provides the ability to add credentials that represent an accepted method of identity. Many online resources such as banking and shopping leverage Google, Apple, Samsung, and Facebook identities which you create for yourself as proof of identity, and the associated credentials can be stored in the digital Wallet.

FACT: Identity and credentials are not the same, which adds to the confusion. **PKOC is a credential, it is not an identity.** PKOC is a credential that originates in your Apple or Android phone, it can be stored in the digital Wallet today on Android phones and in the future may be enabled in the Apple phone's digital Wallet.

Asymmetric (PKI) vs. Symmetric key pairs (Everything else)

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.

What are the costs associated with PKOC credentials?

PKOC credentials either reside in an applet embedded in a plastic card or “badge” OR they reside in a mobile device application found in the Apple or Google play stores. If cards are preferred, some manufacturers already offer smart cards with PKOC applets preprogrammed for approximately $4-$6 MSRP, depending on the quantity.. If the mobile device version is preferred, PKOC credentials can be sourced from a multitude of app providers or as a User, any organization may use the specification to develop their own PKOC credential Application. This clearly puts control into the hands of the “Users.” Today many national and global organizations have their own employee apps which could include a PKOC credential at little or no cost to the organization after development.

What are the differences between today’s mobile wallet-based access credentials vs. a PKOC access credential?

The main difference is that the Wallet credentials of today utilize a Symmetric keyset, while PKOC uses an Asymmetric keyset. Encryption keysets are required to do a “handshake,” which validates that the credential is authentic and prevents cloning of the credential because the key is kept secret and secure.

In a **Symmetric keyset**, both keys are private and must be kept secure, making it very difficult and risky to share either of them.

In **Asymmetric keyset**, one key is private and kept secure while the other is Public and can be freely shared.

How are PKOC and Physical Logical Access Interoperability (PLAI) related?

They are two entirely separate initiatives at PSIA: Simply put, PKOC is the specification that defines a secure credential standard (mobile or keycard) that is generated independently of a third-party credential issuer. (It’s generated within the card or phone) It also defines how device manufacturers can enable devices (readers, locks, control panels, Biometric devices, etc.) to securely consume the credential for purposes of authentication and access verification

PLAI is the PSIA developed specification that defines the mechanism used to securely, electronically share identities, credentials, and access groups from an authoritative identity database (such as Active Directory, Workday, PACS or other data source) with other Physical and Logical security systems. Similar to the way in which commercial PIAM solutions share identities and credentials throughout an organization’s operational systems, except PLAI is an open standard.

PKOC: Elevating the Experience of Secure Credentials

For more information on how to compare PKOC to Wallet based mobile credentials and standard symmetric key smart cards, see table below: **Credentials Comparison Chart**

Functionality/Feature	**Wallet Based mobile Phone Credentials	PKOC Mobile Phone Credentials	PKOC Card Credentials	Other Smart Card credentials using Seos or Mifare or DESFire
Distance for Read	2 inches	2 inches -20 feet	2 Inches	2 inches
Highly Secure	Yes	Yes	Yes	Yes
Transmission method	NFC	BLE, NFC, UWB	NFC	NFC
Interoperable with any devices	Yes	Yes	No	No, must be a device with matching keyset
Requires you to download an App	Most	Yes		No
Requires you to keep App running to use credential	No	Yes	No	No
Same credential works with various manufacturer products	*No Requires multiple credentials in the wallet	Yes, Single credential works on all PKOC enabled devices	Yes, single credential will work on all PKOC enabled devices	No, must be a device with matching keyset
Any credential will work with any device	No- device must be same technology as the credential issuer due to the symmetric key methodology	Yes	Yes	No Seos will only work with Seos, Mifare and DESFire will only work with a device containing the matching symmetric key
*Cost	$10-$30/Year	$0*	$4.00 - $6.00 per card, one-time fee	$4.00-$6.00 per card- one-time fee
Available formats for access badge	Any	Public Key 64 – 256 bits	Public key 64-256 Bits	Any
Requires third-party issuance	Yes	No	Card only – credentials are created within the card	Yes
Works without phone battery charged	Yes	No	N/A Card is passive - No battery required	N/A these cards are passive, no battery required
Uses NFC	Yes	No	Yes	Yes
Uses BLE	No	Yes	No	No
Uses Symmetric or Asymmetric Key Pair?	Symmetric	**A**symmetric	**A**symmetric	Symmetric
Anyone can offer this credential type	No	Yes	Yes	Only if it's a unique, User owned encryption keypair.

*Note: for each credential in the wallet there will be a per/user/year fee

** While current Wallet credentials are associated with symmetric encryption key sets, -future Wallet credentials may evolve to utilize Asymmetric encryption methodology.