PKOC & PLAI: Elevating the Experience of Secure Credentials

The Latest Buzzzzzzzz

The latest buzz in access control is about something called PKOC, pronounced /ˈpēˌkäk/ (like peacock). PKOC is an acronym for Public Key Open Credential. PKOC represents an openly available specification, written and supported by the Physical Security Interoperability Alliance (PSIA) and its Secure Credential Interoperability (SCI) Working Group. Conforming to the IT Industry Standard for Public Key Infrastructure (PKI), it's 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.

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 the public key becomes the "badge #" which can be easily shared with any system or device used to control access. With PKOC the USER literally "owns" the encryption keys and does not require any complicated process for managing or sharing keys. Furthermore, PKOC enables you to "Bring Your Own Credential" (BYOC).

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

Why will there be a push to have mobile access credentials stored in the Apple or Google Wallet?

This is only necessary if a third-party provider is issuing symmetric encryption keys because the provider knows both keys, which is an inherent risk. There are some additional benefits to storing your access credential in the digital wallet which is addressed in the matrix. If you use a private-public key methodology, where the encryption keys originate in YOUR device and the private key remains private and secure within your phone or card, then the digital wallet becomes a moot point from a security perspective, albeit other conveniences.

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

The wallet-based access credential is generated and issued by a third-party App & credential provider, then "added to the wallet", (i.e., the secure element in the device), similar to the way you "Add to Wallet", your airline boarding pass. **The PKOC access credential** is generated within YOUR device's secure element, using a third-party App only to trigger the keygen function, therefore it is not necessary to store it in the digital wallet, it is born there. **The digital wallet** transmits the credentials over Near Field Communications (NFC). Whereas **the mobile phone PKOC credential** transmits using a Bluetooth Low Energy (BLE) method. While NFC works more consistently across the various mobile phone devices, it requires the device to be very near to the field of communication so you must take the phone out of your pocket or backpack and present it within 2" of the reader for it to work. Due to restrictions imposed by Apple and NXP on NFC transmission, PKOC credentials currently are only available using BLE on a phone device but NFC in plastic card form factor. While the PKOC card has a similar read range, i.e. 2", the PKOC mobile phone credential has a variable, configurable read range anywhere from 2 inches to approximately 20 feet, which can significantly enhance the user experience.

PKOC & PLAI: Elevating the Experience of Secure Credentials

Digital Wallet mobile credentials vs. PKOC mobile credentials Comparison Chart

Functionality/Feature	Wallet Based mobile Access Credentials	PKOC Mobile Credentials
Distance for Read	2 inches	2 inches -20 feet
Highly Secure	Yes	Yes
Transmission method	NFC	BLE, NFC, UWB
Interoperable with any devices	No	Yes
Requires you to download an App	Most	Yes
Same credential works with various manufacturer products	No. Requires multiple credentials in the wallet	Yes. Single credential works on all devices
Any App will work with any device	No	Yes
Cost	$6-$10/Year	$0*
Available formats for access badge	Any	Public Key 64 – 256 bits
Requires third-party issuance	Yes	No
Works without phone battery charge	Yes	No

*Note: Some manufacturers may charge a fee for app usage which includes PKOC, but PKOC is a free protocol.

Asymmetric (PKI) vs. Symmetric keys (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 yours. 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 nobody, (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 risk of compromising the credential. For this reason, it is extremely simple AND interoperable, no strings attached. Any manufacturer you wish to work with may request the PKOC specification from PSIA and enable their devices to read that credential.

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

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 device) 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 specification that defines the mechanism used to securely, electronically share identities & credentials from an authoritative identity database (such as Active Directory, Workday, PACS or other data source).