Physical Security Interoperability Alliance

Secure Credential Interoperability (SCI)
Working Group

PSIA

Physical Security Interoperability Alliance

MISSION:

IDENTIFY EXISTING AND EMERGING STANDARDS RELEVANT TO THE PHYSICAL SECURITY INDUSTRY, WORK TO ENHANCE THEM TO SUPPORT INDUSTRY REQUIREMENTS AND ENCOURAGE THEIR ADOPTION BY OUR MEMBER COMPANIES AND THE INDUSTRY. IN ADDITION, THE GROUP WILL REVIEW AND MEET SPECIFICATIONS THAT ARE SUBMITTED AS OPEN STANDARDS.

*PHYSICAL SECURITY INTEROPERABILITY ALLIANCE PSIA is headquartered in **SANTA CLARA, CA**, and is a 501(c)(6) organization.*

PSIA

Secure Credential Interoperability (SCI) Working Group

The Genesis of the Secure Credential Interoperability WG

- In 2014 Hugo Wendling, CEO of WaveLynx Technologies, designed the LEAF architecture to enable an interoperable smart card credential. The design is based on DESFire EV2 & EV3 chip technology.
  - It is currently supported by a consortium of manufacturers in response to extraordinary commercial access control end user demand. www.LEAFIdentity.com

- In 2020 Mohammad Soleimani, CTO of Kastle Systems & active member of PSIA, defined the Public Key Open Credential (PKOC) architecture and proposed this as a possible industry standard to achieve secure encrypted access credential interoperability without dependence on a single source product such as DESFire chips. Mohammed Soleimani is Chairman of the SCIWG.

Contributing Technology

BLUETOOTH LOW ENERGY (BLE)- PKI enabled BLE access devices

NEAR FIELD COMMUNICATION (NFC) - Capable on all PKI enabled NFC access devices

SMART CREDENTIALS & DEVICES - Android devices, iOS devices and NFC devices (Smart Cards, Smart phones, Wearables, Smart Fobs)

CONNECTIVITY - Wiegand (For access point verification only), OSDP or Ethernet

Definition Page (For the purpose of this paper)

- **Access Device** – Online Reader, Wireless Locks, Biometric reader
- **BID –** A term commonly used to mean the unique "ID Badge Number" stored in the Access Control System
- **NONCE** - a random or semi-random number that is generated for a specific use, typically related to cryptographic communication or information technology. ... Typically, a **nonce** is some **value** that varies with time, in order to verify that specific **values** are not reused.
- **OSDP** – Open Supervised Device Protocol an access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products. https://www.securityindustry.org/industry-standards/open-supervised-device-protocol/
- **PACS** - Physical Access Control System
- **PKI** – Public Key Infrastructure – Asymmetric, highly secure encryption method requiring an authoritative certificate database (the Infrastructure).
- **PKOC** – Public Key Open Credential – Asymmetric encryption method NOT requiring the Infrastructure but just as secure
- **PLAI** –Physical Logical Access Interoperability- A standard interface to an electronic access control system database.
- **Smart Device** – Phone, Tablet, Wearable, Card, Fob
- **Secure Credential** – The Private & Public Key created by the smart device
- **Wiegand-** a wiring & communications standard used on access control card readers and systems, that has become the most common de faction communication method for such systems since the 1980's

Secure Credential Interoperability (SCI) Working Group

What is it?

Why is it needed?

Why and How does it work?

What's in it for you?

What Are Our Goals?

DEFINE a universally compatible secure credential for the physical access control industry in the form of cards, fobs, mobile devices & wearables.

LEVERAGE the security, flexibility and convenience of Public Key Infrastructure (PKI) and NEGATE the need for investment in the infrastructure.

INCREASE the adoption rate of Mobile Credentials for access control.

ENABLE entire access control ecosystems to easily utilize an INTEROPERABLE credential.

Why Is This Important NOW?

PROXIMITY CREDENTIALS (125 KHz) are not secure and organizations are migrating to a secure credentials NOW.

SMART CARDS are secure but pose extremely challenging interoperability issues.

MOBILE CREDENTIALS are gaining in popularity but also present interoperability issues.

THE DEMAND IS HIGH.
Commercial environments need high security AND interoperable credentials and are investing in solutions today.

How Is This Made possible?

- A unified, interoperable credential is made possible by leveraging **existing standards & commercially available technology:**
- Most smartphones **enable the Public/private key to be created by the device.** This is compatible with nearly all the smartphones produced over the last 5 years.

NIST based ECC P-256 Public/Private Key generation (Add link to reference doc FIPS186 Section D.2.3) Digital Signature Standard (DSS)

- **Over The Air (OTA) transmission** such as cellular or wifi enables the Public Key to be provisioned as the Badge ID to the necessary access devices. The Public Key is exchanged OTA, while the Private Key never leaves the originating Smart device.
- **The public key becomes the Credential** - BRILLIANT!

Why Does It Work?

IT IS PKI - WITHOUT THE “I”

This solution eliminates the barriers associated with the Infrastructure component of Public Key Infrastructure methodology.

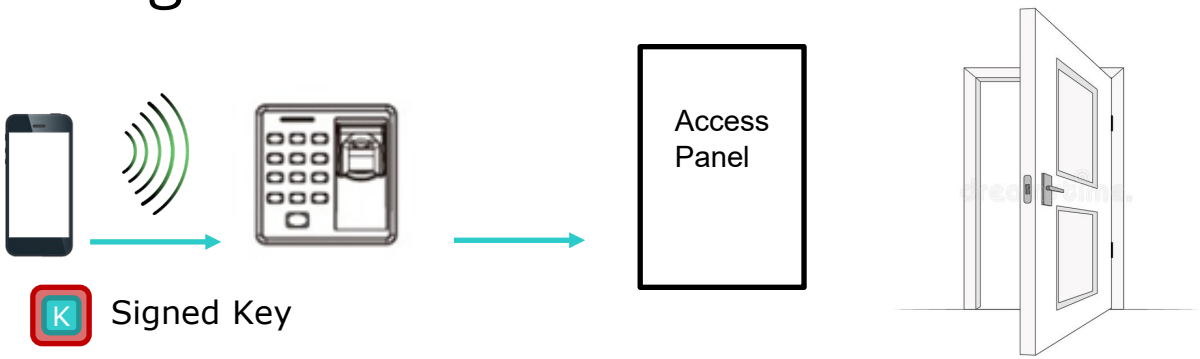
How Does this Work?

Here is summary of the architecture in **4 STEPS**:

1. The Public Key and Private Key are BOTH generated by the phone (smart device) when the App is activated.
2. The Private Key remains in the phone (smart device) and becomes the verification key.
3. The Public Key is pushed OTA to an enrollment server then passed through to the PACS via a PLAI connection, effectively becoming the badge ID in the PACS User record.
4. The PACS automatically pushes the Public Key to all connected access devices (i.e. access panels, access readers, intelligent locks, biometric devices, etc.)

Summary

When the phone is presented to an access device it is authenticated at the device or at the access panel (PIV model) then the public key (acting as the BID) is pushed to the PACS for access granted.

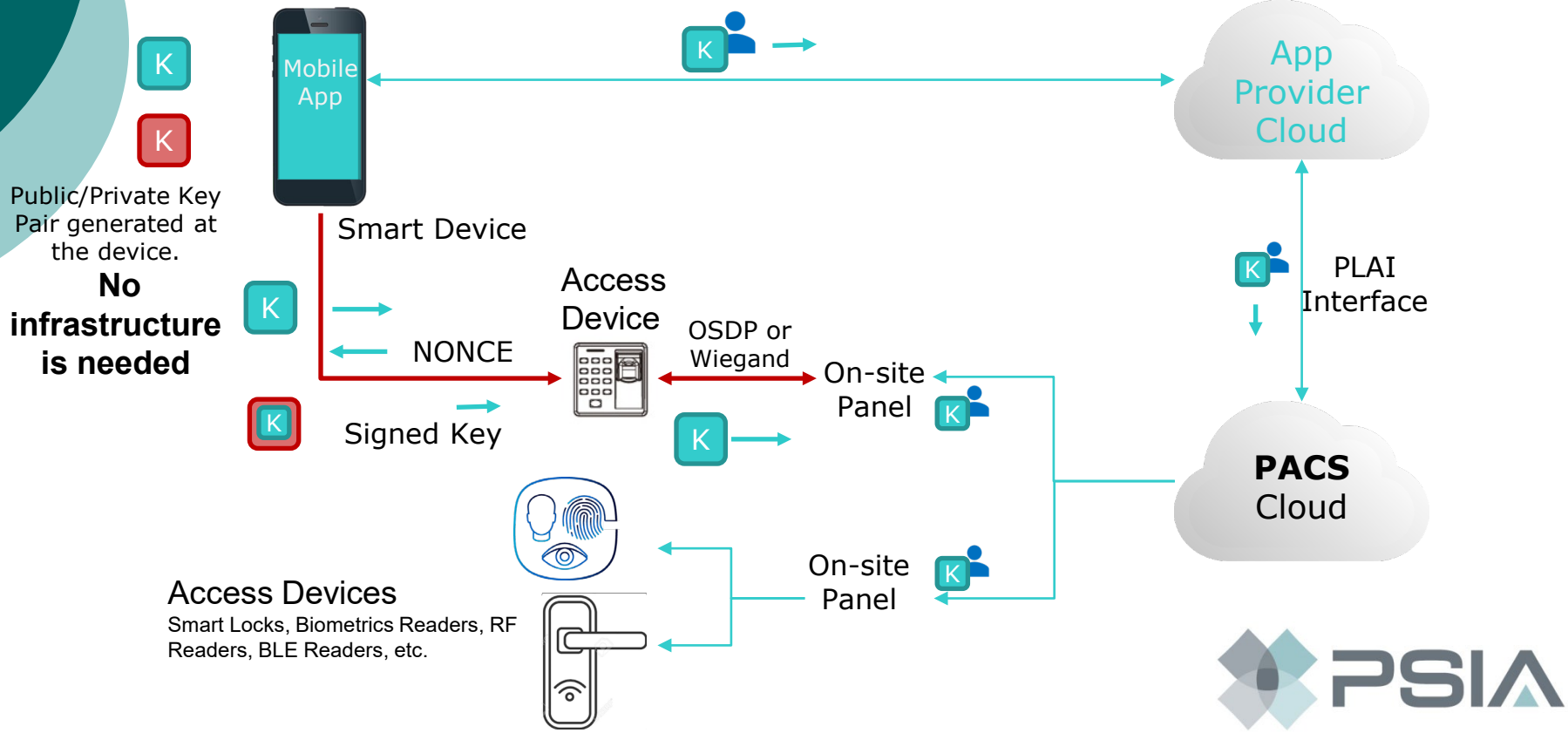


Noteworthy:

This does not require management of any site key or Facility Codes on any of the devices

SCI Architecture

Challenge/Signature verification performed at the **EDGE**

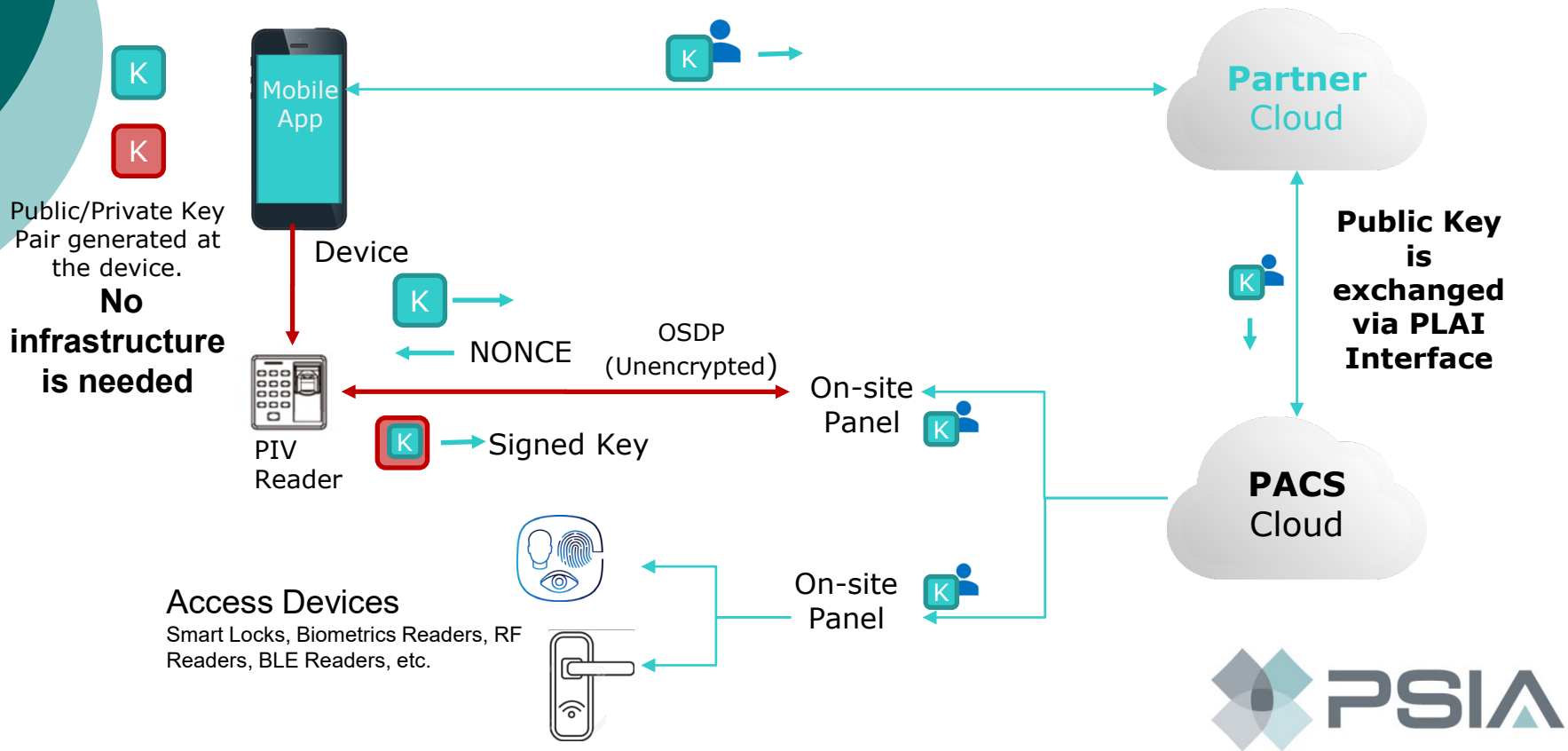


PSIA

Secure Credential Interoperability (SCI) Working Group

SCI Architecture

Challenge/Signature verification performed at the **Panel** (PIV Architecture)



PSIA

Secure Credential Interoperability (SCI) Working Group

PUBLIC KEY OPEN CREDENTIAL (PKOC)

PSIA

Secure Credential Interoperability (SCI) Working Group

Participating Members

ALLEGION

ASSA ABLOY

dormakaba

Farpointe Data
Readers • Credentials

IDEMIA
augmented identity

Johnson Controls
tyco

KASTLE SYSTEMS

LENEL·S2

WaveLynx
technologies corporation

PSIA

Progress So Far

SOLVED FOR BLE - Fully defined architecture for devices with BLE & compatibility

TECHNICAL SPECIFICATIONS - A detailed technical specification has been drafted

PROOF OF CONCEPT - POC testing is in the planning stages

PUBLIC KEY OPEN CREDENTIAL (PKOC)
What's In It For You?

- ★ **Pioneer** a new Mobile Credential standard that is highly secure, simple to manage, easy to use and cost effective
- ★ **Steer** the requirements to ensure your products can adapt
- ★ **Be first to Market** with a Mobile Credential solution that is interoperable with other prominent market leading brands
  - PSIA member adoption = immediate broad range adoption and interoperability
- ★ Product **sales skyrocket** as Mobile credential adoption grows
- ★ The current global supply chain issues and chip shortage will likely drive **fast paced Mobile adoption** as we return to the office

Interested parties are WELCOME!

Participate as a PSIA member

Contact: David Bunzel dbunzel@sccg.com