Physical Security Interoperability Alliance

PRESS RELEASE
October 10, 2024

PKOC Bluetooth 3.0 Released

Enhanced Cryptography Support

The Physical Security Interoperability Alliance (PSIA) announced its Public Key Open Credential PKOC Bluetooth 3.0 specification at GSX 2024. This is the culmination of a significant amount of work from some of the leading access control companies in order to achieve this milestone. The 3.0 spec features enhanced cryptography, which supports all Bluetooth hardware. In addition, the spec has been optimized to reduce the time it takes to authenticate.

“The PKOC technical committee represents all facets of the access control industry, with considerable experience and perspective.” said David Bunzel, Executive Director of the PSIA, “Collaborating to achieve a truly open specification has benefited from this impressive base of knowledge.”

The simplicity of PKOC, ease of integration, and the significant advantage of asymmetric encryption were some of the drivers that are most interesting to consultants, Integrators, and customers.

“PKOC 3.0 maintains security from the credential to the ACS using industry standards,” said Jon Torre, Sr Director of Applications Engineering for ELATEC. “This is the next logical step in interoperability and security.”

Vendors and customers appreciate the platform flexibility and interoperability that PKOC offers. "We are excited to support PKOC from PSIA as it provides a path for Access Control vendors to deliver interoperable products for mobile credentials over Bluetooth. PKOC enables EMS Integrators’ (EMSi) vision to deliver mobile apps on iOS and Android and readers for mobile credentials, logical access, mapping and location-based services on a flexible and interoperable platform" said John Tepley, CEO at EMSi.

PKOC creates truly secure and interoperable credentials. The commercial and security advantages of the asymmetric key based credential over traditional symmetric keys which have been used for decades is

finally attainable with the PKOC standard. A public key-based solution cannot be underestimated in its value over traditional credential solutions.

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).

The PKOC Bluetooth 3.0 spec is now available at this link.

###

For Media Inquiries contact:
David Bunzel, PSIA Executive Director, 1.650-938-6945, dbunzel@psialliance.org

Notes to Editors:

●PSIA is a 501(c)6 organization created to define, recommend and promote standards for IP-enabled security devices and systems.
●PSIA was founded in February of 2008 and incorporated in March of 2009.
●The Physical Logical Access Interoperability (PLAI) specification was introduced in 2013.
●The PKOC specification was introduced in 2021

PSIA | info@psialliance.org | www.psialliance.org

STAY CONNECTED