CRAYONIC
SECURE DIGITAL IDENTITY

Crayonic Badge™

Specification of version B1.0

Version 1.3, 08/2022

Identity & Access

Crayonic Badge™ (CB) is a smart wearable device in a badge holder form factor for securing digital transactions in online and offline environments. CB implements multiple open standards with well-defined protocols and enables highly secure identification and authentication of its owner in a range of use cases.

The Badge secures all sensitive personal information such as biometric templates, cryptographic keys, FIDO2 credentials, and X.509 certificates. With this data, the user can interact with other devices and applications.

Multiple authentication factors on-device

Identification and authentication of the user are based on knowledge and biometric factors, thus meeting the triple factor authentication criteria for high-security use cases - possession, knowledge, and inherence. Version B1 supports static biometrics (fingerprint) and the knowledge factor (4-digit PIN code). Future versions of CB will support additional static (face) and behavioral biometrics with dynamic characteristics such as the user's gestures, body motions, and voice. Processing of biometrics and PIN verification takes

place on the device and within a secure environment of the authenticator, without dependence on external resources or connectivity.

On-body detection & gestures

In the firmware update planned for Q4 2022, the CB authenticator will support on-body detection, enabling continuous authentication. Embedded motion sensors will keep the user logged into the authenticator while wearing it. In case no motion is detected for a defined period of time (i.e. 15 seconds), the user will be logged out of the CB authenticator. Additionally, the motion sensors are used for gestures (e.g. double tap) to confirm the user's intent to access a nearby device/desktop/IoT.

Proximity login & logout

Crayonic Badge smart authenticator enables auto login and logout via a specifically designed Bluetooth-USB dongle called Crayonic Bridge (CBLE). The Bridge requires no additional software or drivers installed on the end-point devices. It serves as a "virtual cable" connecting the PC with Crayonic Badge or Crayonic KeyVault authenticators over secured Bluetooth protocol.

Configuration & manageability

Crayonic Badges can be managed and configured using Crayonic's open source enterprise-level access management and a single sign-on solution Crayonic Gateway.

Core Specifications - Crayonic Badge™ model B1

Authentication protocols	FIDO2, PIV over USB, BLE, NFC, Crayonic Bridge BLE (CBLE)
Optional alternative authentication schemes*	OATH-TOTP, OATH-HOTP, custom OTP schemes - over USB or out-of-band
Biometric verification factors	Fingerprint (up to 5 templates), FAR < 1:50 000 , FRR < 1:20
Optional alternative biometric verification factors*	Gesture, Voice
Protection mechanisms	Secure Element for cryptographic operations; Key storage; Trust root and certified TRNG. Certified against Common Criteria EAL5+ profile.
Key management features	FIDO resident key management with master entropy secure backup; (Optional) PIV key and X.509 certificate issuance; Key/value storage;
Cryptographic algorithms	ECDSA P-256, SHA-1, SHA-2, AES-256, HMAC, RSA 2048

Secure display	128x32 px OLED (for transaction confirmation, OTP and on-device management)
Audio feedback	(Optional) Beeper*
Mechanical protection	Waterproof, shock-proof,
Sanitization	Hospital disinfectants and cleaning agents (alcohol, chloride)
Temperature ranges	Operation: 0 °C to 50 °C, Storage: -10 °C to 55 °C
Battery	Rechargeable LiPo min. 300 mAh. Average expected duration - 3 to 6 months per charge.
Communication standards	NFC - ISO 14443; USB - ISO 7816/CCID, BLE 5.0
Physical port	USB-C
Mass Storage	AES encrypted (32MB - 64MB FAT16/32)
Manufacturing standards	Auditable secure manufacturing in the European Union (Slovakia); RoHS
Certifications	FIDO2 Level 1, Microsoft Azure AD, Secure Element Common Criteria EAL5+, CE
Dimensions	max. 90 mm x 65 mm x 7 mm (29g)

See also Crayonic KeyVault Technical & Security Whitepaper

Use Cases & Compatibility Table

Use Case	**Support**	**Connectivity**
Badge personalization		
Fingerprint, PIN code authentication	on-device	-
Gesture, Voice authentication*	on-device	-
Badge settings & security policies	on-device, Crayonic Gateway, Mobile App*	
Passwordless biometric login		
to a PC over FIDO2, U2F	Windows 10 1903+ with MS Azure AD/hybrid	USB, BLE, NFC, CBLE
to a PC over PIV (X.509)	Windows 7+, Linux*, Mac OS 10.12+	USB, NFC, CBLE* (Windows)
to a web service over FIDO2	Windows 10 1903+ (Edge, Chrome, Firefox, Brave)	USB, BLE, NFC, CBLE

	Linux, Mac OS, ChromeOS	USB, CBLE
	iOS Safari	USB, NFC, CBLE*
to a web service over U2F	Android	USB, BLE, NFC, CBLE*
to a web service with X.509 client certificate over PIV	Windows 7+, Windows 10 (Edge, Chrome, Brave)	USB, NFC
FIDO2 credentials backup & recovery via Crayonic Gateway	Windows 10+, Linux, Mac OS	USB, BLE, CBLE*
Certificate issuance (X.509)		
Locally	Windows 7+ using the Crayonic PIV Manager app	USB
Remotely over FIDO2 via Crayonic Gateway	Windows 10+, Linux, Mac OS 10.12+	USB
Mass storage		
AES128 encrypted (min. 30MB) FAT16/32	Windows 7+, Linux, Mac OS 10.12+	USB, CBLE*
Digital signing		
Locally using X.509 certificate over PIV	Windows 7+, Linux, Mac OS	USB, CBLE*
Cloud e-signing over FIDO*	Windows 7+, Linux, Mac OS	USB, BLE, NFC, CBLE
Physical Access		
ISO 14443 standard	N/A	NFC
HID SEOS, MIFARE DESFire protocols*	N/A	NFC
OTP (per request TOTP, HOTP...)*	on-device	stand-alone, USB
Enterprise Password Management		
Bitwarden, LastPass, KeePass, 1Password integration*	Windows 7+, Linux, Mac OS	
Blockchain		
Signing ETH transaction*	Windows 7+, Linux, Mac OS	

* Functionality planned for H1 2023 unless re-prioritized based on demand


St. Martin
Nicky Cra
Registered
iversity Hospital
urse