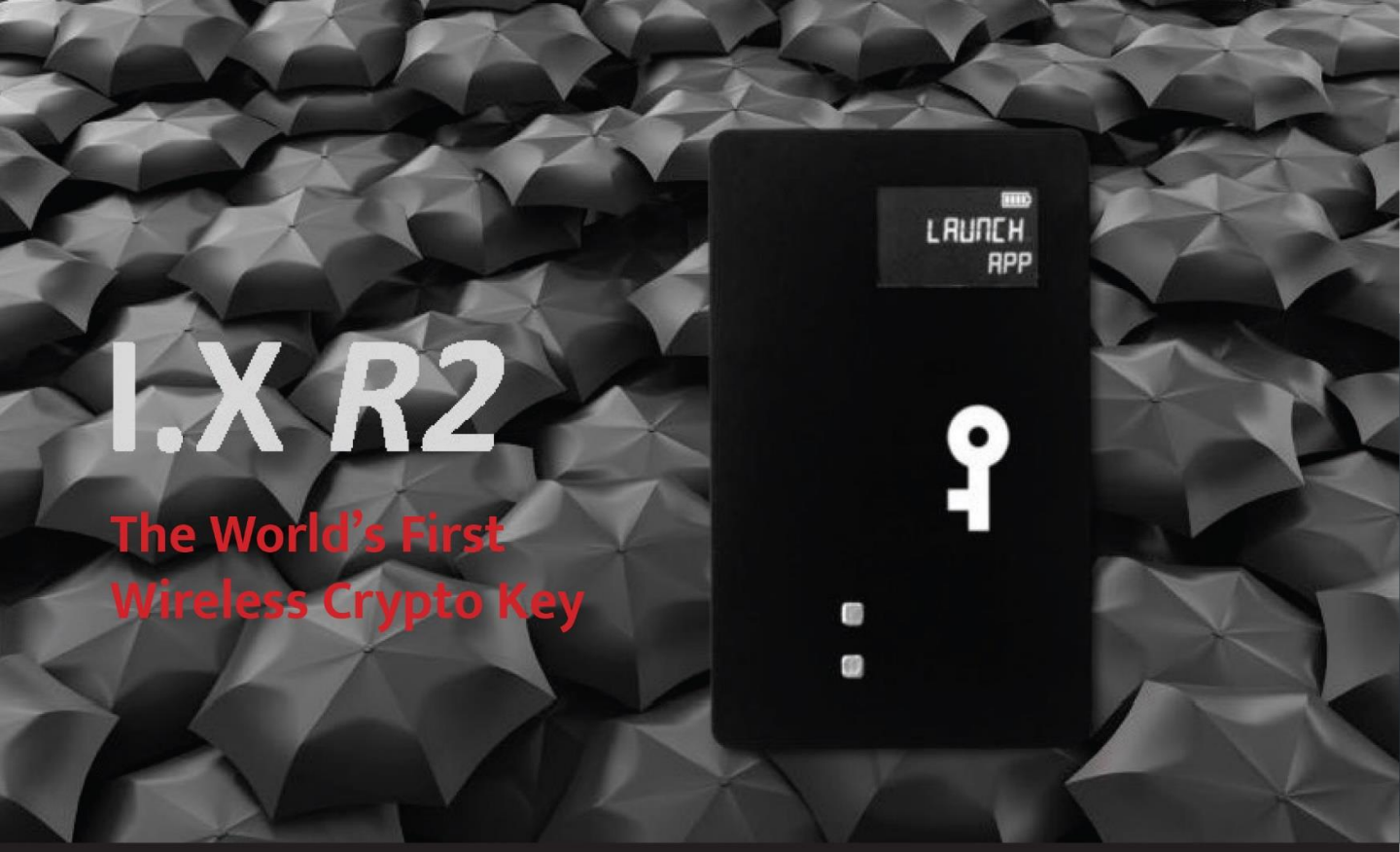


Secures The Privacy Of Your Conversations

The I.X R2 is a credit card sized Wireless Privacy Key that secures the privacy of your communications . It uses patented technologies to encrypt all types of conversations and to authenticate its users. The I.X R2 is compatible with iOS and Android smartphones and it requires no IT effort at all to install or provision , which makes it a suitable solution for companies of all sizes .

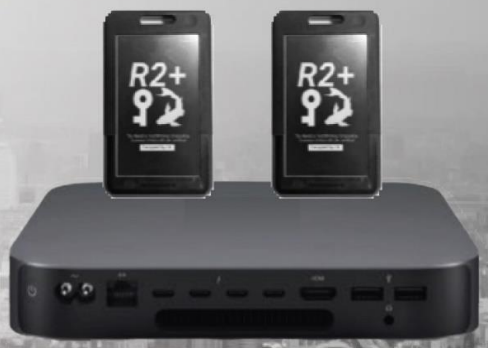
The encrypted wireless connection between the I.X R2 and your smartphone gives you full control over your privacy. Using the I.X 3 way authentication™, the R2 is a secure communication solution that works without password thus excluding what is considered to be the weakest link in anyone's security.

The I.X R2 is easy to setup and use. Just create an account via the I.X R2 app on your phone. Connect your I.X R2 Wireless Privacy Key to your phone to create the 3 way authentication™ and you are ready and secure. If you lose your phone, your data will be locked automatically as the key disconnects outside the vicinity of your phone. The I.X R2 itself contains a CC EAL5+ certified secure chip and is linked with your mobile phone through an encrypted Bluetooth connection. This means no encryption key will be stored on your open OS smartphone!

To create a direct, peer to peer communication channel two I.X R2 Wireless Privacy Keys negotiate a session key independent from a server! The I.X R2 manages vital elements of your security outside your smartphone to avoid risks. This beats any software only solution.

I.X Solution Comparison

	I•X		WeChat		LINE
HW PROTECTED KEY (OWN YOUR KEY)	V				
END TO END ENCRYPTION	V	V	V	V	V
P2P BROADCAST	V				
SECURE FILE STORAGE	V				
SECURE CALL	V	V	V	V	V
SELFDESTRUCTED MESSAGE	V				
OFFLINE KEY VERIFICATION	V	V		V	
NO DATA RETENTION ON SERVER	V				
NO ACCESS USER CONTACT LIST	V				



ONWARD SECURITY [CONFIDENTIAL] R2 Mobile Application Security Assessment Report – I.X

1. Executive Summary

Onward Security followed the penetration testing methodology ISECOM OSSTMM and NIST SP800-115 and refer OWASP Mobile Security Testing Guideline (MSTG) and the product usage to evaluate the security level of the secure communication mobile application and its hardware cryptography key developed by I.X during the period from April 9 2018 to May 4 2018.

The 4 different testing scenarios designed by Onward Security include attack from network-side, get either user's phone or key, and get both of user's phone and key are pass the testing.

No	Scenario	Result
1	When hacker is aside without hardware crypto key and user's phone	Pass
2	When hacker gets user's phone without hardware crypto key	Pass
3	When hacker gets user's hardware crypto key without user's phone	Pass
4	When hacker gets user's hardware crypto key and user's phone and return to the user	Pass

Source: Onward Security

Trusted 3rd party lab certified I.X security platform

BUREAU VERITAS 1828

BUREAU VERITAS