MobileIDWorld

Industry News ◂ prev next ▸

Search ▸

Maintaining Secure BYOD: GO-Trust Offers Military Strength Encryption To Business Customers

Peter Counter / February 27, 2014

SHARE

One of the big struggles in businesses of all sizes right now is the troubling question of how to handle the encroaching bring your own device (BYOD) attitude that is encroaching in on day-to-day operations. Taking a big picture view of the situation, BYOD can be extremely positive, allowing for increased efficiency and better work-life integration. With the benefits come risks however, without good policies and the proper technology, BYOD might as well stand for data compromise.

Poor mobility habits are even putting federal agencies at risk, according to a recent study by Cisco. Thankfully, the technology is available to turn what could seem like a major security liability into nothing but opportunity.

To this effect, GO-Trust Technology Inc, currently attending both the Mobile World Congress and RSA Security Conference 2014, announced recently that its SDencrypter microSD has achieved FIPS 140-2 level 3 certification from NIST.

What this means is that users in government and corporate environments working with Android or Windows smartphones have an encryption solution certified for US military use. It can protect data such as mission critical files being sent peer-to-peer, confidential messages and even voice calls.

“GO-Trust is the only company providing FIPS 140 certified peer to peer communication on smartphones, tablets and other SD card enabled devices,” says Darren Lee, Go-Trust’s CEO. “This means companies can have complete control over the mobile environment of their employees with the confidence of military-level security, even with BYOD users.”

The SDencrypter has synergy with GO-Trust’s Sycret Voice App, which, when combined with the FIPS 140 microSD solution allows for increased functionality. Users with SDencrypter inserted into the microSD slot on their smartphone can download the app from Google Play and then set up an encryption tunnel that scrambles all outgoing media sent to other Android devices with the same security set up.

GO-Trust describes the effect as the epitome of stealth communications. Each call, text or email is sent over data channels, leaving not even a phone number that can be recorded to log the origin.

According to the company, even if both phones involved in an encrypted transaction are compromised the information cannot be recreated. This is because a random encryption key is generated for every conversation made. It’s kept on the SDencrypter itself, where every encryption operation takes place. Nothing happens in the open, nothing can be subpoenaed or hacked.

GO-Trust is currently actively looking for distribution partners in Canada and the United States.

Tags: Mobile Security Voice

By Peter Counter

RELATED POSTS ◂ ▸

Sponsors

ImageWare Systems
ImageWare Systems is a leading provider of multi-Modal biometric user authentication, patented agnostic plug-n-play technology that promotes interactive communication and Out-Of-Band authentication on mobile platform.

Northstar Recruiting
Northstar uses their industry knowledge to recruit top talent for Biometric and Identity Management companies.

ZK Teco
ZKTeco is one of the leading providers of security and time management solutions in the world. We provide one-stop service to global business partners and customers.