

[Company](#)[Contact](#)[Vormetric](#)[Blog](#)[English ▾](#)**THALES**

Thales e-Security

[SOLUTIONS ▾](#)[PRODUCTS & SERVICES ▾](#)[PARTNERS](#)[SUPPORT](#)[KNOWLEDGE BASE ▾](#)[Home](#) > [About Thales e-Security](#) > [Press](#) > [News](#) > Accenture Integrates Blockchain Technology with Thales Hardware Security Module to Address Key Risks for Financial Services, Government, Healthcare and Other

» News & Information

Visit us regularly to stay abreast of our latest news, coverage, and general information as well as exciting market trends and developments!

February 8, 2017

Accenture Integrates Blockchain Technology with Thales Hardware Security Module to Address Key Risks for Financial Services, Government, Healthcare and Other

NEW YORK & LONDON & HONG KONG - Accenture (NYSE:ACN) has unveiled a patent-pending solution that simplifies the ability of blockchain technology to integrate with the industrial-grade security systems that support sectors including financial services, healthcare and government. The solution creates a developer-friendly interface between emerging blockchain platforms and widely used hardware security technology. Accenture cooperated with Thales – whose hardware is currently used by most major banks globally to secure records and assets from cybertheft – to develop the solution.

[Click to tweet:](#) #Blockchain integration w/@Accenture uses @thalesecurity HSMs <http://bit.ly/2lkbCRx>

Hardware security modules (HSMs) are crypto-processors that securely generate, protect and store digital keys. Keys stored in the Thales HSM architecture cannot be extracted or used except under a highly controlled protocol. The new solution is based on the widely used nShield HSM developed by Thales and creates a simple path to large-scale commercial use of blockchain technology.

“Blockchain is quickly maturing across industries and is set to profoundly change how businesses operate,” said Simon Whitehouse, senior managing director and head of blockchain technologies at Accenture. “But current applications cannot meet the high security standards of most mission-critical IT infrastructure. That is because the digital keys used to secure and validate messages and transactions historically have proven vulnerable to network attacks. Our solution provides the same kind of physical security that banks have relied on for decades to keep money and transaction records safe from cyberthieves. It will clear a wider path not only for banks but for governments, insurers, healthcare providers and others to do real-world deployments of blockchain technology.”

Currently, blockchain-based systems typically rely on “cyberwallets” to store digital keys

Contact Thales e-Security

email: sales@thalessec.com

tel:

Americas +1 888 744 4976 or +1 954 888 6200

EMEA +44 (0) 1223 723600

APAC +852-2815-8633

News Archive

[2017](#) | [2016](#) | [2015](#) | [2014](#) | [2013](#) | [2012](#)
| [2011](#) | [2010](#) | [2009](#) | [2008](#)

for blockchains. But because those keys typically reside on software servers, they can become vulnerable to network breaches of the kind that have occurred on cryptocurrency exchanges in recent years. The solution makes it extremely difficult if not impossible for digital keys to be misappropriated because they are stored in physical isolation from IT networks and are architected with highly sophisticated, deterministic security mechanisms. In addition, the platform need only be installed once, allowing companies to secure each of their blockchain applications using the same solution – regardless of which blockchain software or application they use – versus crafting a code interface for each solution.

Jon Geater, Chief Technology Officer at Thales e-Security said, “The possibilities for blockchain are endless. In the financial sector everything from transactions to contracts and deeds could use a blockchain to legitimize and simplify the settlement process, and industries such as healthcare and federal government also stand to benefit from this technology. However, in order for blockchains to work, we need to believe and trust them, which means every participant must agree and anticipate how they will take part in the chain. Unfortunately innovation and vulnerability very often go hand-in-hand. Accenture has built trust and security into the technology of the chain itself, using Thales HSMs to protect the chain and prevent any nefarious activity. Thales continues to invest in blockchain delivering the ‘root of trust’ to this emerging technology.”

“The opportunity to benefit from blockchain technology within sectors like financial services and healthcare depends on an ability to protect digital keys using conventional standards of security,” said David Treat, managing director, financial services blockchain lead at Accenture. “While there have been bespoke blockchain integrations with HSMs before, this solution offers a simpler and more flexible standard to connect blockchain platforms with the leading HSMs. We are committed to delivering these types of real-world innovations that will serve as the stepping stones to make blockchain technology a reality for large-scale enterprises.”

The solution used Fabric, a Hyperledger technology and can be adapted for other leading blockchain technology platforms. Hyperledger is a global, open source collaborative effort of more than 100 major companies focused on advancing cross-industry blockchain technologies.

Solution highlights

Many security-conscious institutions rely on HSMs to safeguard and manage their digital keys and protect things like ATM machines, mainframe operations, point-of-sale (POS) machines and to verify and sign SWIFT messages – they are used in virtually any application that requires secure, verified digital signatures. While most people have no idea of the role of an HSM in securing sensitive information, it’s a technology used every day. For example, HSMs in a bank’s data center are used to validate your PIN when you withdraw cash from an ATM, or validate the transaction cryptogram when your purchase goods at a merchant POS terminal – in both cases only the HSMs under the bank’s control have access to the correct keys to perform the secure processing. Some of the benefits of an HSM include:

- **Keys are stored within secure HSM boundary:** the keys always live inside the secure, certified HSM boundary vs. in software or on a hard drive where they are vulnerable to attacks.
- **Tamper-resistant hardware:** FIPS 140-2 Level 2 and 3 certified HSMs are tested to stringent standards and are extremely difficult to access by unauthorized users.
- **Sophisticated cryptography:** HSMs use a certified, cryptographically secure random number generator to create keys, providing superior quality keys than a typical computer system.

About Thales e-Security

Thales e-Security is the leader in advanced data security solutions and services, delivering trust wherever information is created, shared or stored. We ensure that company and government data is secure and trusted in any environment – on premise, in the cloud, in data centers and in big data environments – without sacrificing business agility. Security doesn’t just reduce risk, it’s an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and meeting the highest standards of certification for high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization’s digital transformation. Thales e-Security is part

of Thales Group. www.thales-esecurity.com

SOLUTIONS

- > By Business Issues
- > By Technology Focus

PRODUCTS AND SERVICES

- > Hardware Security Modules
- > Key Management Systems
- > Identity Management
- > Network Encryption

PKI CONSULTING
BLOG
SUPPORT
PARTNERS
CONTACT US

CAREERS
COMPANY
COOKIES
LEGAL
PRIVACY POLICY



Thales Group

2017 Thales e-Security, Inc., all rights reserved.