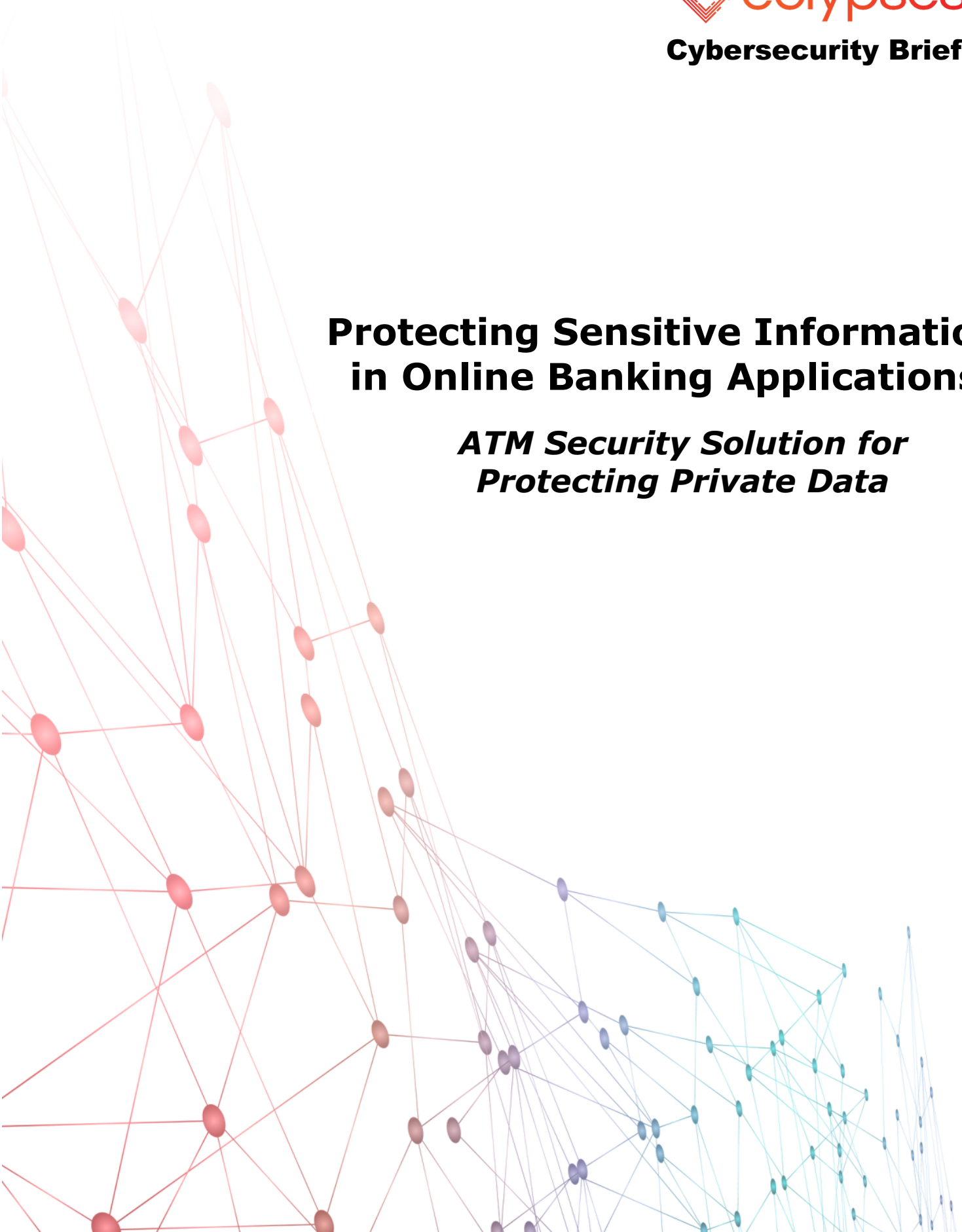
eclypses™

Cybersecurity Brief

Protecting Sensitive Information in Online Banking Applications

ATM Security Solution for Protecting Private Data



Introduction

Automatic Teller Machines, or ATMs, are in the news a great deal lately, but the publicity isn't positive. Cybercriminals are increasingly breaching the security of ATM networks and hitting a bonanza, fittingly known as "Jackpotting".

Picture a thief in front of a slot machine and not feeding it any money, and instead cash rapidly flows out into their hands. This is what's happening with ATM networks more and more, and the amount of currency that's stolen is massive.

The techniques that are currently in place to stop these criminals are not enough and fall far short. Current defensive and detection methods just aren't working. It's inevitable; cybercriminals will find a way to get into the systems and ATMs as well as other devices. The solution is MicroToken Exchange™ (MTE). MTE can prevent currency theft when an attack does happen – by making data Invisible

What Makes MicroToken™ Technology Smarter

MicroToken Exchange (MTE) is a security framework that provides an extreme level of end-to-end privacy, protecting commands in motion to both connected and intelligent devices.

MTE is built upon the idea that "if real commands continue to be hacked, lost, or stolen, then stop using real commands; use MicroTokens Instead!"

A MicroToken replaces real data as a placeholder. The MicroToken is created through a proprietary form of artificial intelligence, created by Eclypses. This is where the real magic takes form.

Here's how it works: two or more devices or endpoints on the network need to be successfully initialized - identifying that the devices are paired - creating a secure one-to-one relationship. This pairing ensures that only the receiving device component is capable of effectively executing the intended command. Each device is then allowed, if applicable, to both send and/or receive data (or commands) back and forth between them.

MicroTokens can only be interpreted by paired points or devices and are meaningless to cybercriminals should they be intercepted.

Valid MicroTokens are hidden within complex "digital chaff", which are false randomized tokens. Thousands of digital chaff are generated each second to hide the useable MicroToken that represents the real data or commend. Plus, the amount of digital chaff is ever-changing as a configurable element of MicroTokenization®.

Adding to Eclypses unbreakable security is the fact that MicroTokens become instantly obsolete. Each time a command is authorized, with or without permission, the entire library of commands is instantly wiped clean and re-initiated on all sides simultaneously. There

are also added layers of protection and schemas that add to the invisible shield that the Eclypses' solution provides.

Up to now, most security architectures did not consider that a cybercriminal could gain physical access in the manner it is now occurring. This changes the game!

With MTE properly deployed, not only are communications to and from an ATM secured, but communications and commands within an ATM are secured as well. This is accomplished in ways that were never before possible.

The MTE security architecture changes the way connected and intelligent devices are secured. This is critical with the rise of the Internet of the things for consumers and industrial control.

Real Business Results

With three patents pending, the MicroToken Exchange framework is as unique as it is secure, providing real business differentiation.

- Secure connection to third party services and your customers
- Removes ability of intruders to detect any value from storage or transmission
- Millisecond operational speeds that do not alter user experience
- Small footprint as standard encryption is not required
- Requires NO key management
- Can be rapidly installed with just the insertion of a few lines of code
- Minimal processing power needed
- In many cases, no changes to hardware are required

About Eclypses

Eclypses offers industry leading cybersecurity solutions that provides the highest level of data privacy available. The company's patent pending MicroToken Exchange technology™ eliminates the need to transmit or store real data. The core technology was initially deployed for use by a Fortune 25 company to protect commercial data as well as payment processing and continues to be utilized for that purpose today.

Contact Eclypses to learn more about MicroToken Exchange today

For inquires: email Info@eclypses.com or call 719-323-6680