Giesecke+Devrient

Trend report

“Alexa, how secure are my digital financial services?”

Banks need to ask themselves that same question as they broaden the channels of access to digital services, argues Gabrielle Bugat, Head of Division for Financial Solutions at Giesecke+Devrient (G+D).

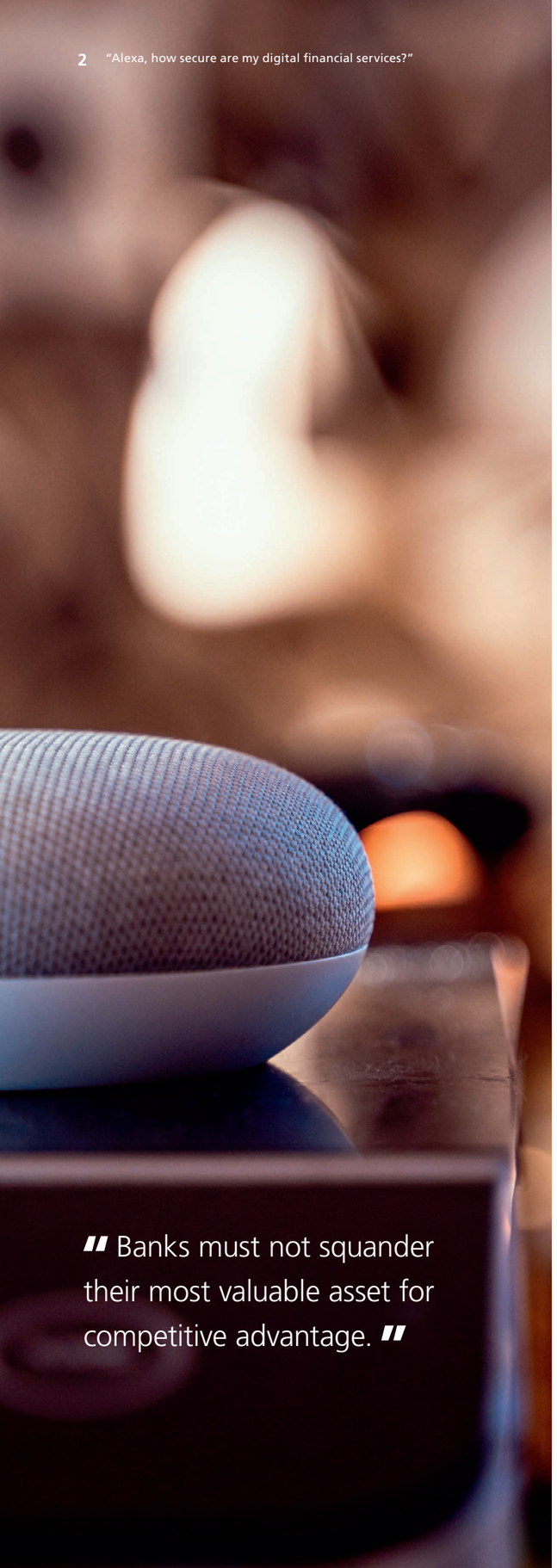
Big banks and financial companies are further enhancing their digital services through virtual personal assistants (VPA) such as Amazon’s Alexa, Apple’s Siri, and Google’s Assistant. Customers in the United Kingdom and United States, as well as in more than five countries in Asia-Pacific can now check their balances, pay bills, and in some cases even send money with voice-activated commands.

More countries and digital services are set to follow. Yet, while this enhances the digital offerings of banks and makes sense from the standpoint of a competitive edge, the ability to undertake sensitive financial tasks through a smart speaker, such as the Amazon Echo that connects to Alexa, raises security issues.

Asking Siri to play a song or Google for a restaurant recommendation is one thing, but it’s another issue when it comes to sharing sensitive personal information. VPAs and smart speakers are new, developing technologies and using them for financial tasks offers another possible entry point for cyber criminals.

At present, Amazon and Google dominate the smart home virtual assistant market and provide open-platform systems that make them well suited to utility needs. Alexa and the Google Assistant can each control more than 5,000 smart home devices from thousands of brands, and the number of supported languages and features offered is continually expanding. Gartner forecasts that, by the end of 2020, end-user spending on VPA-enabled wireless speakers will reach $2.1 billion.

> “ Alexa and the Google Assistant can each control more than 5,000 smart home devices from thousands of brands. ”



" Banks must not squander their most valuable asset for competitive advantage. "

MAINTAINING THE TRUST

The challenge for banks is not to squander one of their most valuable assets in the rush for a competitive advantage. Historically the banking business is built on trust and even as customers increasingly open up to data-driven digital and mobile services, they want to be assured that personal data will be protected.

To ensure they maintain and increase customer trust in this age of digital banking, financial service providers need a smart, customized IT strategy that transparently ensures the security of all digital access services. Given the diverse array of devices used to access banking apps, it is critical that security not be limited to one area, but that a holistic approach be adopted as the system architecture of devices offers diverse attack points for cyber criminals seeking to steal data or run frauds and scams.

On the physical side, devices can be hacked over the storage and SIM cards, the flash or ramdisk memory, USB connection, wireless interfaces such as GPRS Bluetooth and NFC, as well as hardware interfaces and firmware. On the logical side, devices are susceptible to attacks on the operating system, malicious third-party apps, remote management hacks, browsers, communication services such as email and SMS.

The most fundamental critical aspects of a comprehensive security strategy for digital services is to protect the source code of the banking programs and ensure secure communication with the back end including the encryption. White box cryptography(WBC) is an essential technology when it comes to minimizing security risks for open devices.

Devices have to be secured to avoid being analyzed or rooted. WBC enables operation to be performed securely without revealing any portion of confidential information. Without WBC, attackers could easily grab cryptographic keys used for making payments from memory or intercept critical information.

In addition, a holistic approach ensures that the environment in which an app is running is also secure. For example, apps must be prevented from being copied or cloned from one device to another. Digital fingerprint touch-id technology can help identify if there quest is coming from the original device and that the device is in a secure operating state.

LIFECYCLE MANAGEMENT

Fundamental to the security approach is lifecycle management. In addition to protective measures on the devices themselves, an extra security component is provided on the server side to ensure the app is comprehensively managed over its lifecycle. For example,this ensures that updates are installed safely, and customer credentials securely managed.

The desire of banks to be a front-runner in providing powerful, new attractive digital financial services needs to be carefully balanced against the need to ensure the security of those services. While digital banking services may ensure a decided competitive edge, banks need to maintain the trust that has been fundamental to the success of their business model. Only a holistic strategy and well-integrated approach to security across all devices will convince customers to continue to trust financial service providers in this age of digital disruption.

" Spending on VPA-enabled wireless speakers will reach $2.1 billion. "

Future Banking – It is all about Securing Payments!

Did you know? Giesecke+Devrient (G+D) technology is unconsciously used by billions of people every day! With more than 700 global Banks putting their trust in G+D and our offerings, we enable secure and convenient transactions for everyday usage.

Founded in 1852 in Leipzig as a printer of bank notes, now with HQ in Munich, G+D is a global powerhouse in payments - be via cash, card or digital services. Our safe payments technology, elegantly combined with smooth customer experiences throughout the whole customer journey, secures the daily life use of financial services. And also creates customer obsession for our clients!

We are: pioneers in payments, industry leader and innovating partner for the financial sector.

Giesecke+Devrient

Giesecke+Devrient Mobile Security GmbH
Prinzregentenstrasse 159
81677 Munich
Germany

www.mobile-security.gi-de.com/futurebanking
mobilesecurity@gi-de.com

Follow us on: