



Business challenge

To effectively secure data on behalf of its banking clients, Fiducia & GAD IT AG needs an evolving strategy that can help it to cope with emerging cybersecurity threats and increased regulations.

Transformation

Fiducia & GAD IT AG adopted a pervasive encryption strategy involving IBM® security features such as IBM z/OS® data set encryption and IBM Z® Multi-Factor Authentication to ramp up data protection.

Business benefits:

Safeguards

clients' reputations and economic stability by reducing impact of data breaches

Boosts

efficiency through simple management of security and regulatory compliance

Enables

high levels of security without stifling business agility

Fiducia & GAD IT AG

Securing data for millions of banking customers while facilitating business agility

Fiducia & GAD IT AG is the information technology service provider within the Finance Group cooperative in Germany. The company's 4,500 employees serve a client base that includes around 900 Volksbanken and Raiffeisenbanken in Germany, cooperative financial companies, and numerous private banks. Ultimately responsible for supporting more than 82 million customer accounts, Fiducia & GAD manages more than 166,000 banking workplaces and 34,000 ATMs nationwide.

"By combining the security capabilities of IBM Z with other tools and our in-house expertise, we are taking every measure to protect our banking clients' data from compromise."

Peter Winter

Manager, Middleware and Transaction

Systems, Mainframe Platform

Fiducia & GAD IT AG

Share this



Hitting a moving target

The cybersecurity landscape never stands still. Each day attackers invent new ways to probe organizations' systems for weaknesses. This is especially true for the banking sector, which is a top target for cyber criminals. In response, and to give people more control over their personal data, industry regulators continue to release increasingly stringent guidelines such as the Payment Card Industry Data Security Standard (PCI DSS).

As IT service provider to approximately 900 German banks, Fiducia & GAD IT AG is responsible for protecting huge amounts of very valuable data. Peter Winter, Manager, Middleware and Transaction Systems, Mainframe Platform, Fiducia & GAD IT AG, says, "Today, the vast majority of money doesn't exist in any physical sense; it's represented by bits on a machine. The banks that we serve manage a lot of Germany's money, which means that any compromise of their data could affect the economy and their reputations. At the same time, our banking clients have to comply with regulations that are getting stricter all the time, such as BaFin [Germany's Federal Financial Supervisory Authority] and PCI-DSS. There's no simple solution—the only answer is a security plan that never stops developing."



It isn't just external factors that influence Fiducia & GAD IT AG's IT security strategy. New requests from internal users also play a role: the growing demand for application programming interfaces (APIs) introduces vulnerabilities that must be identified and addressed.

Pascal Meyer, Senior Enterprise Architect at Fiducia & GAD IT AG,

adds, "Securing data cannot come at the price of business innovation. We're incorporating approaches such as containerization into our IT landscape and hosting applications in the public cloud where appropriate. The ability to control and encrypt data across an IT environment that is becoming more diverse is essential but challenging."

"It was easy to implement IBM z/OS data set encryption, and we saw benefits immediately, in terms of both time savings and reduced resource consumption."

Pascal Meyer, Senior Enterprise Architect, Fiducia & GAD IT AG

Ratcheting up security

Fiducia & GAD IT AG is building on the exceptional security of its [IBM Z](#) platform, taking advantage of new features to bolster protection of data and systems. Meyer comments, “We’re seeing IBM Z evolve dramatically, turning into an open enterprise server that can host cloud-ready applications managed with Kubernetes and [OpenShift](#).”

Executing a [pervasive encryption](#) strategy on IBM Z, Fiducia & GAD IT AG is applying extensive encryption to data in-flight and at-rest using IBM z/OS data set encryption. As a result, the company has been able to replace self-written encryption and decryption programs for many applications. Fiducia & GAD IT AG is in the process of enabling z/OS Enterprise Readiness Technology (zERT) to monitor and record the cryptographic protection attributes of network connections terminating on z/OS. With zERT, Fiducia & GAD IT AG can determine which of the connections are properly or improperly configured. This could potentially help the company in its efforts to simplify compliance reporting.

Meyer says, “It was easy to implement IBM z/OS data set encryption to enable pervasive encryption, and we saw benefits immediately, in terms



of both time savings and reduced resource consumption.”

For many years, Fiducia & GAD IT AG has relied on the [IBM zSecure suite](#) to automate IBM Z security administrative tasks, implement security policies, detect threats and enable real-time alerts. The company integrated IBM zSecure with [IBM QRadar® Security Information and Event Management](#) to take advantage of embedded intelligence to refine its response to security incidents.

Fiducia & GAD IT AG also utilizes [IBM Hardware Security Modules](#) (HSMs) extensively to perform cryptographic operations and protect keys within a purpose-built computing environment. Using the [IBM Java API for CCA](#) package, combined with interoperability between classical programming languages and Java, the company allows Java (alongside all classic programs on z/OS) to consume z/OS native cryptographic services via one API. To reduce the need for distributed hardware security modules, the company relies on the

[Advanced Crypto Service Provider](#) solution to enable distributed applications to invoke z/OS native cryptographic services remotely.

Fiducia & GAD is deploying [IBM Z Multi-Factor Authentication](#) to implement the strong access control measures typically required by regulations such as PCI DSS. Meyer explains, “Within the next few months, we will fully deploy multi-factor authentication, stepping up the security around access to user accounts on IBM Z.”

In close collaboration with IBM, Fiducia & GAD IT AG evaluates new IBM security capabilities as they are released, and uses these to augment its overall IT security plans. For example, the company is investigating the [IBM Enterprise Key Management Foundation](#) and Trusted Key Entry for Master Key Management to help it to manage keys and certificates.

“We’re demonstrating to our clients that the IBM Z platform is the future for cloud-ready development. Security continues to get better on IBM Z, and so does the ability to innovate.”

Peter Winter, Manager, Middleware and Transaction Systems, Mainframe Platform, Fiducia & GAD IT AG

Delivering benefits to businesses

By securing data on IBM Z, Fiducia & GAD IT AG is protecting its banking clients from the potential reputational damage and financial penalties that can be associated with data breaches. With so many of Germany's banking systems running on infrastructure managed by the company, Fiducia & GAD IT AG helps to ensure service continuity for millions of people.

Winter says, "By combining the security capabilities of IBM Z with other tools and our in-house expertise, we are taking every measure to protect our banking clients' data from compromise. As a result, we contribute to the stability of the German economy."

Meyer continues, "Working with IBM, we can roll out capabilities out-of-the-box that can help us comply with emerging regulations more easily. The IBM Z roadmap is developing alongside our own to help us continue boosting security while making management easier."

Fiducia & GAD IT AG is a partner for innovation for its banking clients. Utilizing open, flexible security features from IBM, the company can safeguard data without curbing business agility. Winter concludes: "We're demonstrating to our clients that the IBM Z platform is the future for cloud-ready development. Security continues to get better on IBM Z, and so does the ability to innovate."

Solution components

- IBM Z®
- IBM® Multi-Factor Authentication on z/OS®
- IBM QRadar® Security Information and Event Management
- IBM zSecure suite

Take the next step

To learn more about enterprise security enabled by IBM Z, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/it-infrastructure/z/capabilities/enterprise-security

Connect with us



© Copyright IBM Corporation 2020. IBM Corporation, IBM Cloud, New Orchard Road, Armonk, NY 10504

Produced in the United States of America, September 2020.

IBM, the IBM logo, ibm.com, IBM Z, and IBM z14 are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.



77035277-USEN-00

