

解决方案：系统软件 行业：银行业

# Fiducia & GAD IT AG

在促进业务敏捷性的同时，确保上百万银行客户的数据安全

在德国，有上百万公民使用并信赖 Fiducia & GAD IT AG 提供的银行服务。为了保护客户数据安全，Fiducia & GAD IT AG 实施了一项普遍加密技术，该技术利用强大的 IBM® 功能，能够降低数据泄露带来的影响，简化监管合规要求，并促进创新。

→ 了解更多信息

## 业务挑战

Fiducia & GAD IT AG 需要不断发展的策略来有效保护银行客户的数据安全，帮助企业应对新的网络安全威胁与越来越多的规定。

## 转型

Fiducia & GAD IT AG 采用了一种普遍加密策略来强化数据保护。这项策略涉及 IBM z/OS® 数据集加密与 IBM Z® 多重验证等多项 IBM 安全功能。

## 成果

维护	提高效率	提高
通过降低数据泄露影响，维护客户名誉与经济稳定	采用方便的安全与法规合规性管理提高效率	在不影响业务敏捷性的情况下提高安全防护级别

## 业务挑战

### 灵活应对变局

网络安全格局从来都不是静态的。攻击者每天都在找新的方法探测企业系统的弱点。银行业是网络罪犯的首要目标，面临的危险尤为严重。为了让客户能对个人数据有更多控制权，行业监管机构不断发布越来越严格的指导标准，如支付卡行业数据安全标准 (PCI DSS)。

Fiducia & GAD IT AG 是一家 IT 服务提供商，为近900家德国银行服务，负责保护大量非常有价值的客户数据。Fiducia & GAD IT AG 大型机平台中间件与交易系统经理 Peter Winter 表示：“如今绝大部分的钱都不是以实体形式存在；而是在机器上用二进制数字表示。我们服务的银行管理着德国许多资金，这意味着任何程度的数据泄露都可能影响到客户的经济状况与名誉。与此同时，我们的银行客户必须始终遵守日益严格的监管，如 BaFin [德国联邦金融监管局] 与 PCI-DSS。面对安全，不存在简单快捷的解决方案，唯一的答案就是永不停止发展的安全计划。”

影响 Fiducia & GAD IT AG 的 IT 安全策略不仅有外部因素。内部用户的新请求也产生了影响：日益增长的应用程序设计接口 (API) 需求引发了各种漏洞，而这些漏洞必须尽快得到识别与修复。

Fiducia & GAD IT AG 高级企业架构师 Pascal Meyer 补充道：“保护数据不能以业务创新为代价。我们正在把诸如容器化等多种方法整合到我们的 IT 格局中，并将应用程序托管在合适的公有云上。在日益多元化的 IT 环境中对数据进行控制与加密的能力非常重要，但是又极具挑战。”

“通过将 IBM Z 的安全功能、其他工具，以及我们的企业专长结合在一起，我们正采取各种措施保护银行客户数据，防止发生泄漏。”

— Fiducia & GAD IT AG 大型机平台中间件与交易系统经理 Peter Winter

## 转型案例

### 稳步提高安全性

Fiducia & GAD IT AG 正在以 IBM Z 平台的卓越安全性为基础，利用新特性加强数据与系统保护。Meyer 评论道，“我们正见证 IBM Z 快速发展成为一个开放的企业服务器，能够托管许多运用 Kubernetes 与 OpenShift 管理的云就绪应用程序。”

在 IBM Z 上实施普遍加密策略时，Fiducia & GAD IT AG 将使用 IBM z/OS 数据集加密对传输中的数据与静态数据进行广泛加密。因此，企业能为许多应用程序更换自写入加密与解密程序。Fiducia & GAD IT AG 正在使 z/OS 企业就绪技术 (zERT) 能够监测与记录在 z/OS 上终止的网络连接的加密保护属性。凭借 zERT, Fiducia & GAD IT AG 能确定连接是否配置妥当。这将会帮助企业简化合规性报告。

Meyer 表示，“实施 IBM z/OS 数据集加密来实现普遍加密很便捷，而且很快能够看到节约时间与减少资源消耗方面的成效。”

很多年来，Fiducia & GAD IT AG 一直依靠 IBM zSecure 套件来自动化 IBM Z 安全管理任务，实施安全政策，检测威胁，并启用实时警报。企业将 IBM zSecure 与 IBM QRadar® 安全信息与事件管理整合到一起，从而利用嵌入式技术来改善对安全事件的响应。

Fiducia & GAD IT AG 还广泛利用 IBM 硬件安全模块 (HSM) 在特定用途计算环境中执行密码操作与保护密钥。利用 IBM Java API for CCA 包，借助经典编程语言与 Java 之间的互操作性，企业允许 Java (与 z/OS 上所有经典程序一起) 通过一个 API 使用 z/OS 本机加密服务项目。为减少对分布式硬件安全模块的需求，企业借助 Advanced Crypto Service Provider 解决方案来启用分布式应用程序，以远程调用 z/OS 本机加密服务项目。

Fiducia & GAD 正在部署 IBM Z 多重验证，以实施 PCI DSS 等法规通常要求的强有力访问控制措施。Meyer 解释道，“在未来几个月内，我们将全面部署多重验证，加强在 IBM Z 上访问用户账户时的安全。”

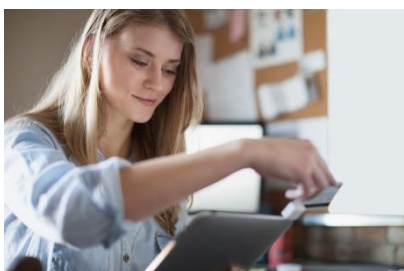
Fiducia & GAD IT AG 与 IBM 密切合作，在新的 IBM 安全功能发布时对其进行评估，并使用这些功能来强化 Fiducia & GAD IT AG 的整体 IT 安全计划。例如，企业正在研究 IBM 企业密钥管理基础与用于主密钥管理的可信密钥输入，以帮助自身管理密钥与证书。

“实施 IBM z/OS 数据集加密来实现普遍加密很便捷，而且很快能够看到节约时间与减少资源消耗方面的成效。”

— Fiducia & GAD IT AG 高级企业架构师 Pascal Meyer

## 成果案例

### 帮助企业获益



通过保护 IBM Z 上的数据，Fiducia & GAD IT AG 保护其银行客户免受与数据泄露有关的潜在名誉损害与经济损失。由于德国许多银行系统都是依靠公司管理的基础设施运行，Fiducia & GAD IT AG 帮助确保百万用户级别的服务连续性。

Winter 说：“通过将 IBM Z 的安全功能、其他工具，以及企业专长结合在一起，我们正采取各种措施保护银行客户的数据安全，防止发生泄漏。这样，我们也为德国经济稳定做出了贡献。”

Meyer 继续道，“与 IBM 合作，我们能推出很多开箱即用的功能，帮助我们更轻松地遵守新的合规性要求。IBM Z 与我们自己的路线图一同发展，帮助我们在简化管理的同时，持续加强安全。”

Fiducia & GAD IT AG 是其银行客户的创新合作伙伴。利用 IBM 开放且灵活的安全功能，公司能够在保护数据的同时不限制业务敏捷性。Winter 总结道，“我们正在向客户表明，IBM Z 平台是云就绪发展的未来。IBM Z 安全性会继续优化，创新能力也会继续提高。”

“我们正在向我们的客户表明，IBM Z 平台是云就绪发展的未来。  
IBM Z 安全性会继续优化，创新能力也会继续提高。”

— Fiducia & GAD IT AG 大型机平台中间件与交易系统经理 Peter Winter



## Fiducia & GAD IT AG 简介

Fiducia & GAD IT AG 是德国金融集团合作社中的信息技术服务提供商。旗下有 4500 名员工，服务的客户包括约 900 家位于德国的人民银行与赖夫艾森银行、合作金融公司与众多私人银行。Fiducia & GAD 最终负责向 8200 多万客户账户提供支持，管理全国 166000 多个银行工作场所与 34000 个自动取款机。

## 解决方案组件

- IBM Z: IBM

## 迈出下一步

要了解有关 IBM Z 企业安全的更多信息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或访问以下网站：[ibm.com/it-infrastructure/z/capabilities/enterprise-security](https://www.ibm.com/it-infrastructure/z/capabilities/enterprise-security)

要了解有关多重验证的更多信息，请访问以下网站：<https://www.ibm.com/products/ibm-multifactor-authentication-for-zos>

要了解有关 IBM zSecure 的更多信息，请访问以下网站：<https://www.ibm.com/security/mainframe-security/zsecure>

要了解有关 Qradar 安全信息与事件管理的更多信息，请访问以下网站：<https://www.ibm.com/products/qradar-siem>

IBM、IBM 徽标、ibm.com、IBM Z 与 IBM z14 是 International Business Machines Corp., 在全球许多司法管辖区域的注册商标。其他产品和服务名可能是 IBM 或其他公司的商标。Web 站点 [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml) 上“Copyright and trademark information”部分有 IBM 商标的最新列表。

本文档为自最初公布日期起的最新版本，IBM 可随时对其进行更改。IBM 并不一定在开展业务的所有国家或地区提供所有这些产品或服务。

本文引用的性能数据和客户示例仅用于说明目的。实际性能结果可能因具体的配置和运行条件而异。本文档内的信息“按现状”提供，不附有任何种类的（无论是明示的还是默示的）保证，包括不附有关于适销性、适用于某种特定用途的任何保证

以及非侵权的任何保证或条件。IBM 产品根据其提供时所依据的协议和条款获得保证。

客户应负责保证遵守适用的法律和法规。IBM 不提供法律建议，也不表示或保证其服务或产品将确保客户遵从任何法律或法规。

良好安全实践声明：IT 系统安全性涉及通过防御、检测和响应来自企业内部和外部的不正当访问来保护系统和信息。不正当的访问可能导致信息被篡改、破坏或盗用，或者导致您的系统遭到误用而攻击别人。任何 IT 系统或产品都不应被认为是完全安全的，并且没有任何单一产品、服务或安全措施能够完全有效地防止任何不当使用或访问。IBM 系统、产品和服务旨在成为合法、全面的安全方法的一部分，它必定涉及额外的操作程序，并且可能需要其他系统、产品或服务配合才能获得最好的效果。IBM 不保证任何系统、产品或服务免受任何一方的恶意或非法行为侵扰，或帮助您企业免受任意一方恶意或非法行为的攻击。