direktzu®: Certified Security

- Data protection
- Availability
- Scalability

At a Glance

- Close cooperation with some of the largest enterprises publicly listed in Germany (“DAX-30”)
- Compliance with all federal data protection regulations
- Comprehensive security standards combined with client autonomy
- Certified server infrastructure provided by Amazon Web Services™ (EC2), e.g. compliant with:
  - Sarbanes-Oxley-Act (United States)
  - Statement on Auditing Standards No.70: Service Organizations, AICPA Type II
  - Payment Card Industry Data Security Standard

direktzu® Meets Highest Client Demands:

SIEMENS

- Integrity, confidentiality and availability of data processing, storage and transmission
- Compliant with Siemens’ “security concept on data management and processing”
- Single sign-on solution based on Entrust GetAccess™

T

- Passed individual threat and risk analysis based on requirements of Deutsche Telekom, the Federal Office for IT Security, and ISO/IEC 27001 guidelines
- Compliant with Deutsche Telekom security protection level 3 (out of 4)
- Single sign-on solution based on Central Authentication Service (JA-SIG CAS)

METRO GROUP
MADE TO TRADE.

- The implementation of METRO Group’s security concept on data processing, access security and documentation
- Single sign-on solution based on SAP NetWeaver Portal™ (SAP Logon Ticket)

W&W wüstenrot
württembergische

- Meets the company’s high demands on data protection, confidentiality and documentation
- Single sign-on solution based on W&W Intranet Portal (Signed URL Redirects)

ONB
OESTERREICHISCHE NATIONALBANK
EUROSYSTEM

- Fulfils the high security demands of a national bank in terms of data protection, confidentiality and integrity

Appendix

I References in More Detail

II Security Standards and Processes

III Network and Server Infrastructure

I References in More Detail

Siemens AG

ϱ direktzu® ensures...

- Compliance with Siemens' "security concept on data management and processing"
- Physical security of buildings and systems
- Security of data and servers
- Access restriction for externally hosted platforms
- Safeguarding of communication against identifiable risks
- Integrity, confidentiality and availability of data acquisition, processing, storage and transfer
- Single sign-on solution based on Entrust GetAccess™

Deutsche Telekom AG

ϱ direktzu® ensures...

- Compliance with the specific security demands of Germany's largest telecommunication enterprise
- Compliance with individual threat and risk analysis based on requirements of Deutsche Telekom and the Federal Office for IT Security (BSI)
- Implementation of all measures required by BSI's IT security manual which is based on ISO/IEC 27001 standards
- Compliance with Deutsche Telekom security protection level 3 (out of 4)
- Single sign-on solution based on Central Authentication Service (JA-SIG CAS)

METRO Group

ϱ direktzu® ensures...

- Compliance with METRO Group’s security concept to guarantee data availability
- Adherence to the company’s high security concept for storage and - if necessary - transportation of data media
- Realisation of METRO Group’s security concept for access security and documentation
- Compliance with a strict organisational scheme with fixed areas of responsibility
- Provision of regular information on data processing and documentation
- Single sign-on solution based on SAP NetWeaver Portal™ (SAP Logon Ticket)

Wüstenrot & Württembergische AG

ϱ direktzu® ensures...

- Compliance with high demands of Wüstenrot & Württembergische AG on data protection, discretion and documentation
- Single sign-on solution based on W&W Intranet Portal (Signed URL Redirects)

Oesterreichische Nationalbank (Central Bank of the Republic of Austria)

ϱ direktzu® ensures...

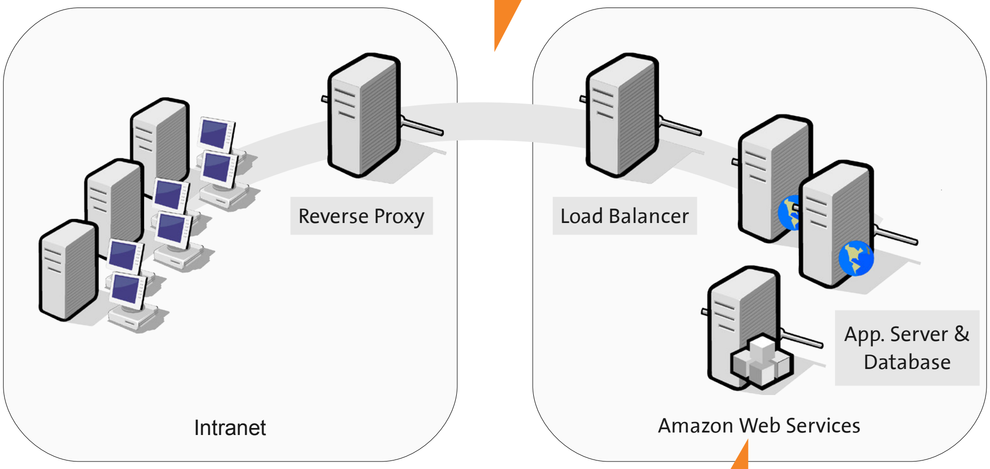
- Compliance with the high security demands of a national bank on data protection, confidentiality and integrity

II Security Standards and Processes

Application Service Provision

- direktzu® uses a reverse proxy solution to guarantee secure access to all web applications. The application is hosted externally and controlled by SSL client certificates.

SSL authentication of the proxy used for encryption and access protection



Servers located in the **European Union** (Ireland)

direktzu®'s Client-Oriented Security Concept

ϱ Developed in close collaboration with some of the largest enterprises publicly listed in Germany (“DAX-30”)

– Meets highest demands on security, integrity and availability

ϱ Provides physical safety and security of all facilities

– Supervision of server systems, non-disclosure agreements with staff, documentation and protection of access to servers

ϱ Restricted access to externally hosted platforms used for internal corporate communication, enforced by

– Access via Reverse Proxy in our clients' intranet

– Secure connection via HTTPS and SSL-Certificate Authentication

– Authentication and authorisation through single sign-on

ϱ Cooperation with certified third party suppliers for data management and processing such as specialised and accredited web host Amazon Web Services™

ϱ Dedicated virtual servers

– On operating system level only accessible through individual, password protected secure shell (SSH) public key authentication

Security Standards

ϱ Amazon Elastic Compute Cloud (EC2)

– direktzu® platforms are being administered and operated by direktzu® on dedicated virtual servers at Amazon Web Services™

ϱ Amazon Web Services™ guarantees...

– Physical safety of its facilities and servers

– Permanent, two-tiered authentication of all Amazon Web Services™ staff

– High level access restrictions and monitoring standards for external personnel

– High security standards as required by internationally accredited certificates

Security Certificates

direktzu®'s service provider Amazon Web Services™...

- Complies with Sarbanes-Oxley-Act (United States) guidelines, including
- Policies on implementation and evaluation of efficient internal control systems and
- Extensive control by the US-American PCAOB (Public Company Accounting Oversight Board)

ϱ Is certified by Ernst&Young to meet the Statement on Auditing Standards No. 70: Service Organizations, Type II of AICPA (American Institute of Certified Public Accountants), including

- Annual reports to verify compliance with security architecture and protective measures according to regulations of the AICPA

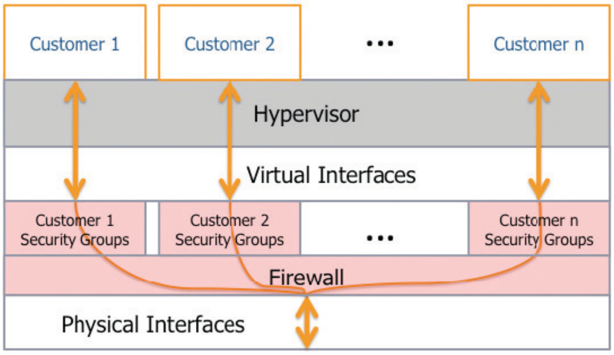
ϱ Complies with the specifications of the PCI (Payment Card Industry), including extensive security regulations by the PCI Security Standards Council - a consortium of the world's major credit card organisations - to ensure the protection of the network

ϱ Is audited based on the PCI Vulnerability Scan involving comprehensive examination of Amazon Web Services™-networks executed by Core Security Technologies, an external service provider using a variety of testing tools

III Network- and Server Infrastructure

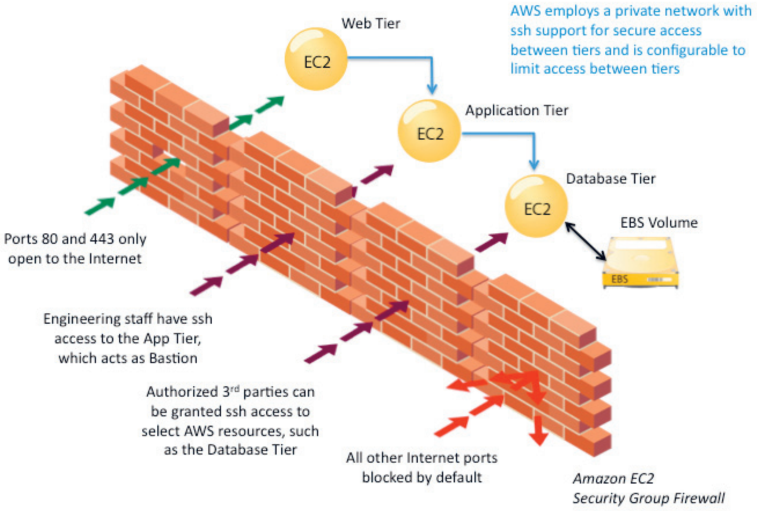
Virtual Servers

ϱ Via Xen™ Hypervisor virtual servers operate isolated from one another on the same physical machine



Source: Amazon Web Services™: Overview of Security Processes, November 2009, p.7

Multi-Staged Security and Access Management


Web Tier
EC2
AWS employs a private network with ssh support for secure access between tiers and is configurable to limit access between tiers
Application Tier
EC2
Database Tier
EC2
EBS Volume
EBS
Ports 80 and 443 only open to the Internet
Engineering staff have ssh access to the App Tier, which acts as Bastion
Authorized 3rd parties can be granted ssh access to select AWS resources, such as the Database Tier
All other Internet ports blocked by default
Amazon EC2 Security Group Firewall

Source: Amazon Web Services™: Overview of Security Processes, November 2009, p.6

Network Security

ϱ The network operated by Amazon Web Services™ is protected against all common threats such as...

- **Distributed Denial Of Service Attacks:** Standard DDoS-techniques such as syn cookies and connection restrictions are in use. In addition, internal bandwidth is larger than the one of the internet service provider.
- **Man In the Middle Attacks:** APIs are accessible via SSL-protected end points supporting server authentication.
- **IP Spoofing:** firewall infrastructure makes sure data traffic with invalid IP addresses is not supported
- **Port Scanning:** Scanning of access ports is a violation of the Terms of Use and is stopped and blocked by Amazon Web Services™
- **Packet Sniffing:** It is technically impossible to receive data traffic of other Amazon Web Services™ users. Attacks such as APR cache poisoning do not work.

direktzu®

Legal advice:

This material is for presentation and informational purposes only and should be treated as confidential. All methods and concepts presented are the copyright of relevantec GmbH. All rights reserved. This material may not be copied, duplicated, reproduced, or used for any other purposes, whether in whole or in part, without the express written permission of relevantec GmbH.