Rohde & Schwarz Cybersecurity

R&S® CYBERSECURITY

SECURING DATA AT REST, IN MOTION AND IN THE CLOUD WITH HIGHEST ENCRYPTION STANDARDS

ROHDE & SCHWARZ

Make ideas real

COMPANY RESTRICTED

R&S® CYBERSECURITY OVERVIEW

ROHDE & SCHWARZ

- ► Independent family-owned company established in 1933 in Munich, Germany
- ► Subsidiaries in more than 70 countries
- ► Revenue of 2.28 billion € (FY 2020/2021)
- ► Around 13,000 employees worldwide
- ► A leading supplier in all business fields

ONE COMPANY, THREE DIVISIONS, DIVERSE MARKETS: WE ARE A RELIABLE TECHNOLOGY PARTNER

TEST & MEASUREMENT

Wireless I Industry, Components & Research I Aerospace & Defense Testing I Automotive

TECHNOLOGY SYSTEMS

Mobile Network Testing I Secure Communications I Critical Infrastructure I Government I IP Network Analytics I Broadcast, Amplifiers & Media

NETWORKS & CYBERSECURITY

Cloud Managed Business I Network & Security Solutions I Certified & High-Grade Crypto Solutions

WHY ROHDE & SCHWARZ CYBERSECURITY?

- One of Europe‘s largest IT security providers
- Part of the Rohde & Schwarz technology group
- More than 30 years of experience in IT security. Cryptography products approved for NATO SECRET-classified information
- Headquartered in Munich, 7 competence centers in Germany and a partner network across Europe
- Award-winning cybersecurity solutions and recognized by industry-leading analysts
- Backdoor-free Policy

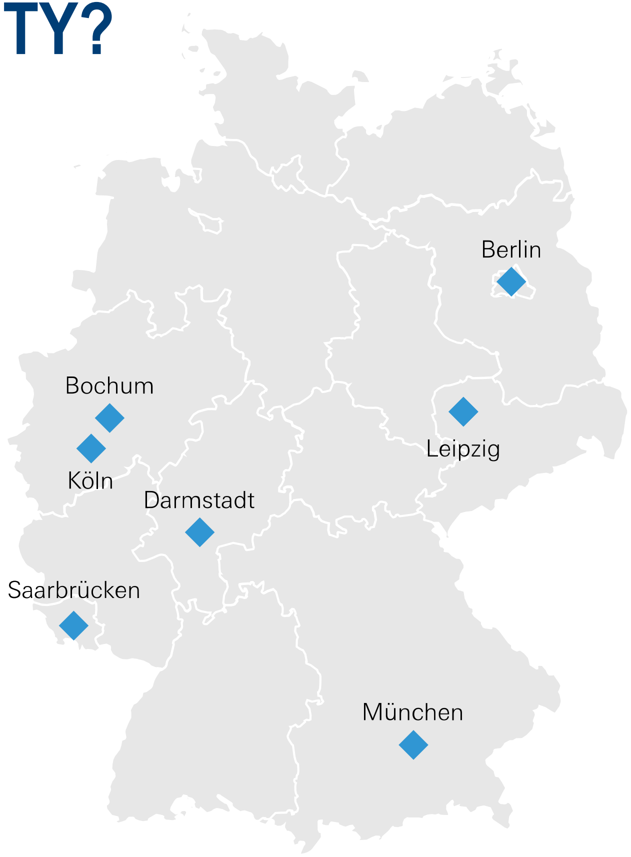
NETWORKcomputing AWARDS 2021 WINNER DATA PROTECTION PRODUCT OF THE YEAR

NETWORKcomputing AWARDS 2021 WINNER NEW SOFTWARE PRODUCT OF THE YEAR

GOLD WEB APPLICATION FIREWALLS (WAF) SECURITY INSIDER AWARD 2021

2021 Computing Security Awards WINNER Security Hardware Product of the Year

2021 Computing Security Awards WINNER Encryption Solution of the Year



CHALLENGES OF A CONNECTED WORLD

SECURITY

- Reliable IT infrastructures form the backbone of every company
- Their manipulation or sabotage can lead to considerable damage

DIGITAL SOVEREIGNTY

- In the digital age, the sovereignty of IT systems and data is essential for the provision of "state of the art" products and services

COMPLIANCE

- Regulatory requirements for IT security and data protection are increasing
- GDPR-compliant use of clouds & collaboration tools

REMOTE WORK

- Digital technologies make it possible to work independently of time and place - for more and more employees part of everyday life
- The security of teleworking is essential

PRODUCT PORTFOLIO

ENDPOINT PROTECTION

- Hypervisor-based remote VPN access for Windows devices
- Virtualized web browsers
- Hard-disk encryption
- Focus on public sector and classified industry (VS-NfD, EU & NATO RESTRICTED)

NETWORK ENCRYPTION

- Layer 2 high-speed group encryption device
- VPN Layer 3 IPsec encryption device
- Focus on public sector and classified industry (VS-NfD, EU & NATO RESTRICTED)

CLOUD SECURITY

- Cloud Data Protection Gateway for DSGVO compliance and protection of sensitive data on MS 365
- In the VS-NfD approval process
- Authorities, NGOs, KRITIS, companies with strict data protection and regulatory requirements or Schrems II dilemma

DATA AT REST ENCRYPTION - R&S®TRUSTED DISK

22.10.2020

R&S® TRUSTED DISK

Trustworthy Disk Encryption

- Full disk and device encryption
- Multi-user functionality with flexible rights management
- Integrated PKI – Central Management
- NATO / EU / German restricted
- Transparent encryption of devices

Technology

- 2-factor Preboot-Authentication
- Crypto Token / Smartcard + PIN
- Centrally managed

NETWORK ENCRYPTION

Product portfolio network encryption

APPROVED NETWORK ENCRYPTION DEVICES

R&S®SITLine ETH NG

- Ethernet encryption
- Transparent integration into ETH services
- Site-to-site
- Crypto and key management in HW
- Full line speed with smallest frames/packets
- German BSI, EU/NATO restricted approved

R&S®Trusted VPN

- Layer 3 / IPsec encryption
- Support for network functions
- Innovative key and SA management
- Site-to-site, client-to-site
- German BSI, EU/NATO restricted approved

Central online security management (TOM)

Central management

R&S®TRUSTED OBJECTS MANAGER FOR ENDPOINT & NETWORK SECURITY SOLUTIONS

- **Usability**
  Central storage of PUKs, user certificates and public keys;
  IPv6-based management; web-based security management client
- **Central network configuration**
  In band management without additional network requirements (routing); minimization of TCP ports for management;
  (1 port - stateful)
- **Security – Cryptography**
  Integrated PKI; ECC with 384 / 512 bit keys; standard curves (Brain pool); online certificate request similar to PKCS #10 standard
- **Network management**
  Smart management; Optimized statistics for monitoring;
  Detailed logging / error messages

SecurITy made in Germany
Trust Seal
www.teletrust.de/itsmig

Network security innovation

OPERATIONAL SCENARIOS

POINT-TO-MULTIPOINT COUPLING VIA LAYER 2 AND LAYER 3 SERVICES

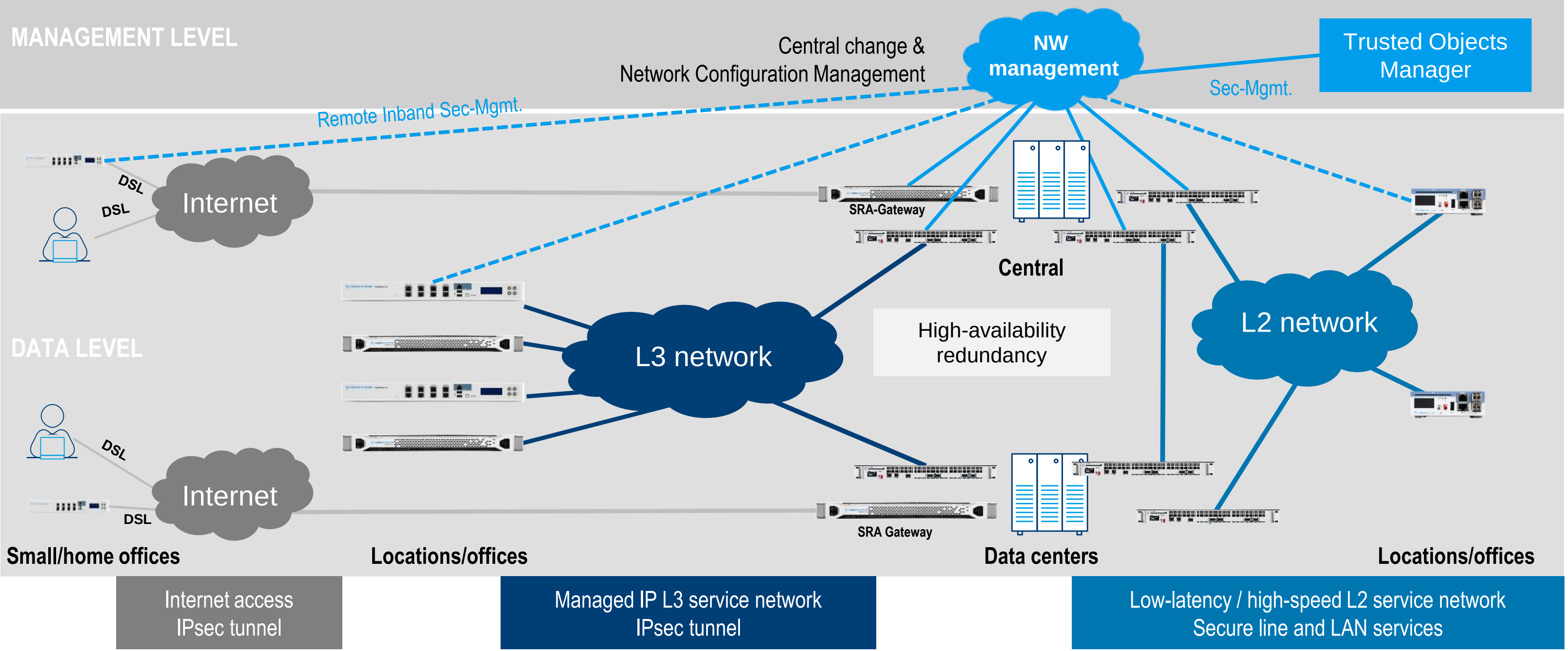
MULTIPOINT FULL MESHING VIA LAYER 2 AND LAYER 3 SERVICES

DATA CENTER COUPLING

CLIENT-TO-SITE: CONNECTION OF DECENTRALIZED SITES (HOME OFFICE VIA LAYER 3)

Network security innovation

UNIFORM NETWORK SECURITY FOR VARIABLE TOPOLOGIES AND TECHNOLOGIES

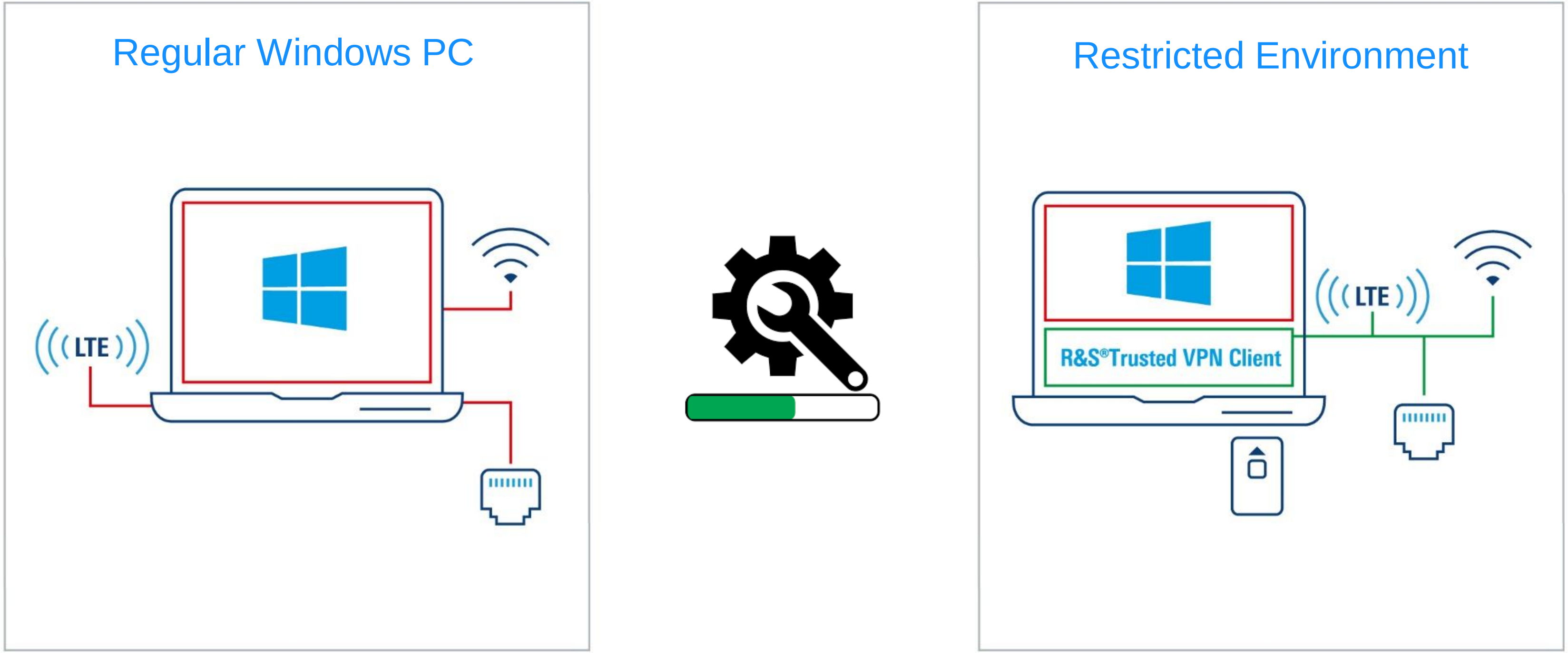


DATA IN MOTION ENCRYPTION - CLIENT-2-SITE ENCRYPTION

SMART-HYPERVISOR VPN CLIENT

BEFORE INSTALLATION

AFTER INSTALLATION



Regular Windows PC

Restricted Environment

SMART-HYPERVISOR VPN CLIENT

- No special hardware needed - compatible with existing devices
- Rollout with existing software deployment solutions via msi package
- Installation on existing Windows 10 OS - no OS redeployment necessary

Panasonic

Microsoft Surface

roda solid IT-solutions

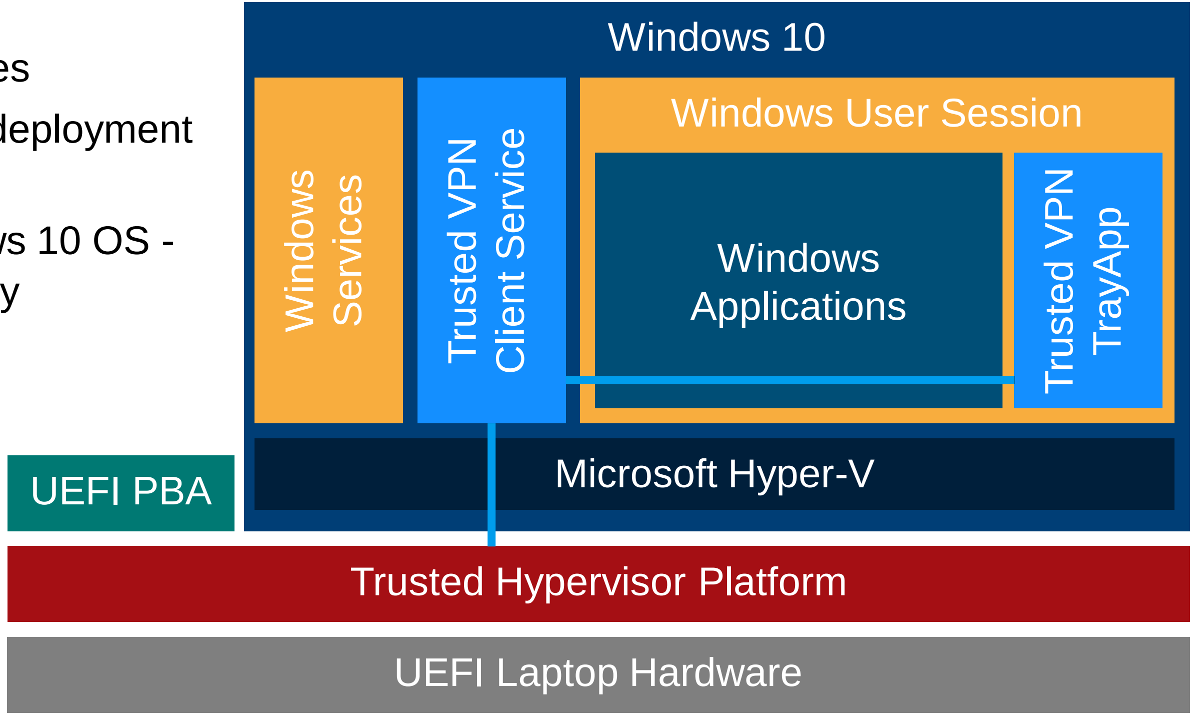
FUJITSU

acer

Lenovo

DELL

hp



Windows 10

Windows Services

Trusted VPN Client Service

Windows User Session

Windows Applications

Trusted VPN TrayApp

UEFI PBA

Microsoft Hyper-V

Trusted Hypervisor Platform

UEFI Laptop Hardware

USE CASES:

Tasks:

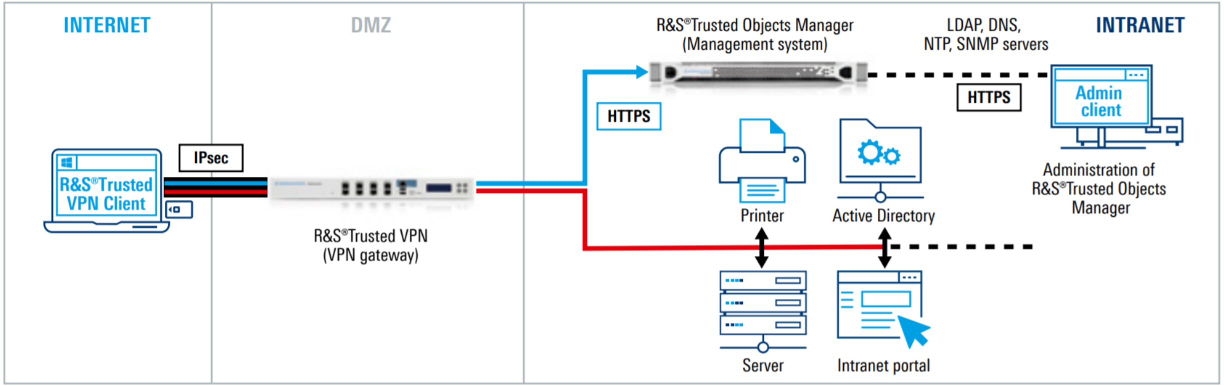
- Replace external hardware VPN solution or weak commercial solutions
- Homeoffice for users who handle confidential information
- Prevent data loss
- Prevent attacks via hardware (BIOS/UEFI)
- Prevent attacks via untrusted LAN, WIFI & LTE connections

Solution:

- T-VPN Software Client

References:

- State Governments
- Police
- Military



R&S®Trusted VPN Client infrastructure

IMPACT OF QUANTUM COMPUTING

IMPACT OF QUANTUM COMPUTING ON CRYPTOGRAPHY

- Key sizes of symmetric algorithms must be doubled (minimum to AES256)
- Asymmetric algorithms (e.g. RSA, elliptic curves) can be "easily" broken
  - 20% probability that RSA-2048 can be broken in 2030 (Mosca, BSI)
  - Save now, decrypt later

CUSTOMER VIEW

Effects all areas of modern digital communication

eCommerce	Online Banking eTrading	Browsing Cloud Services
DRM / Streaming	Secure Messaging	SSL Certficates Trust Provider
Virtual / Remote Desktop	DNSsec	Internet of Things 5G

IMPACT OF QUANTUM COMPUTING ON CRYPTOGRAPHY

Possible approaches to hardening

1. Post-Quantum-Cryptography (PQC)

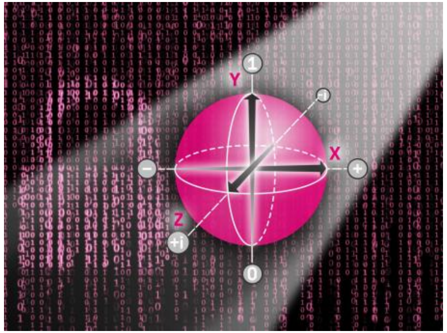
- “classic” algorithms that can be implemented in software/firmware
- based on additional assumptions: not information-theoretically secure

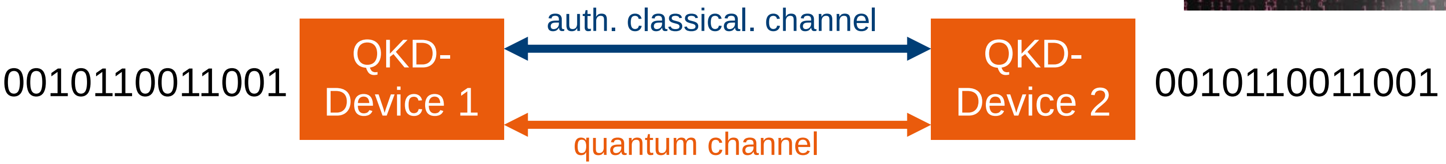
2. Quantum Key Distribution (QKD)

- The only method that has been proven to be secure so far, even against as yet unknown attacks
- Distance currently limited to 100 km (Dark Fiber)

WHAT IS QUANTUM KEY DISTRIBUTION (QKD)?

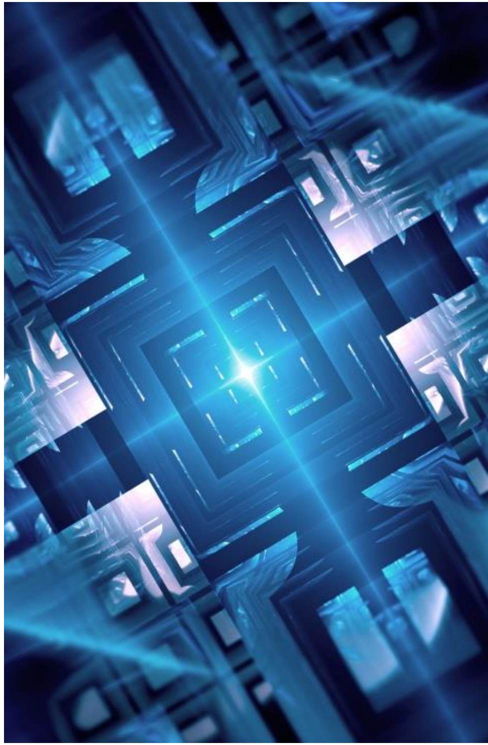
- **Symmetric key exchange between 2 parties using quantum mechanical methods**
  - Safely based on the laws of nature instead of limited computing power or algorithms
  - Single or entangled photons as carriers of quantum mechanical properties
  - Quantum mechanical coherence of the transmitted signals (no quantum computer!)
  - Long-term security, independent of computing power
  - Implicit protection against eavesdropping
  - Dedicated quantum channel between endpoints
  - Authenticated (classic) channel between endpoints





WE ARE RESEARCHING TODAY TO DEFEND AGAINST THREATS OF TOMORROW

- In order to maintain highest security standards in the future, research is currently being conducted into post-quantum cryptography and quantum key exchange.
- We provide our cryptological expertise and our experience in building and implementing secure devices and systems to numerous research projects. Together, we are driving research into the encryption of the future.
- Excerpt
  - HQS: Hardware-based quantum security
  - OPENQKD: Collaboration in European research projects
  - QuNET: Pilot network for quantum communication in Germany
  - Integration of further measures in devices

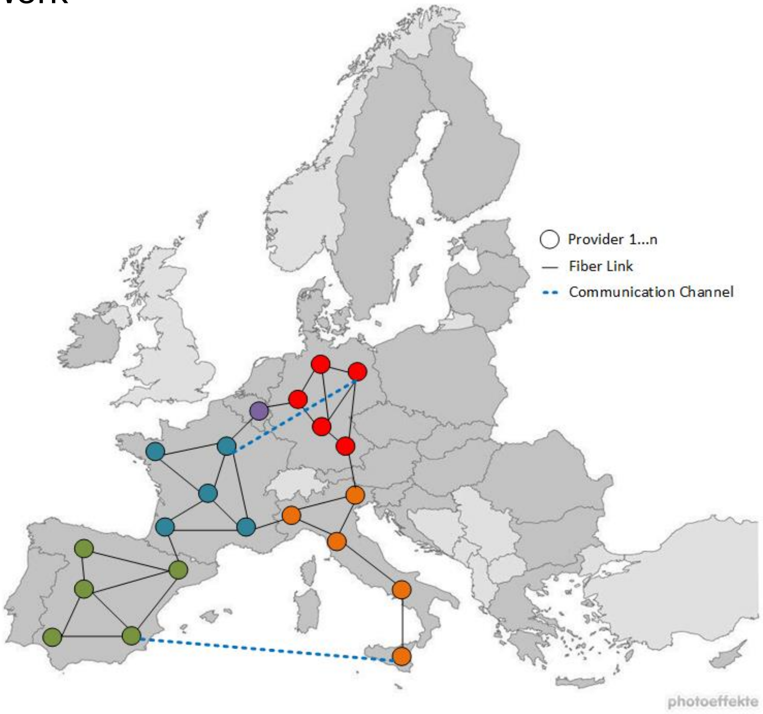


QUANTUM-SAFE COMMUNICATION

EuroQCI: The European quantum-safe communication network

- ► Several hundret millions of funding

- ► E.g. EU Secure Quantum Communication Infrastructure
  - 108M€ for the development
  - 44M€ for the deployment



QKD MARKET STATUS – TIME TO ACT!

► **QKD Technology is about to be marketed**

- Startups and publicly funded projects have proven their fundamental function
- First larger practical operations expected in the next 24 months
- First devices available (based on COTS components, large & expensive)
- Technology can still be scaled and miniaturized significantly

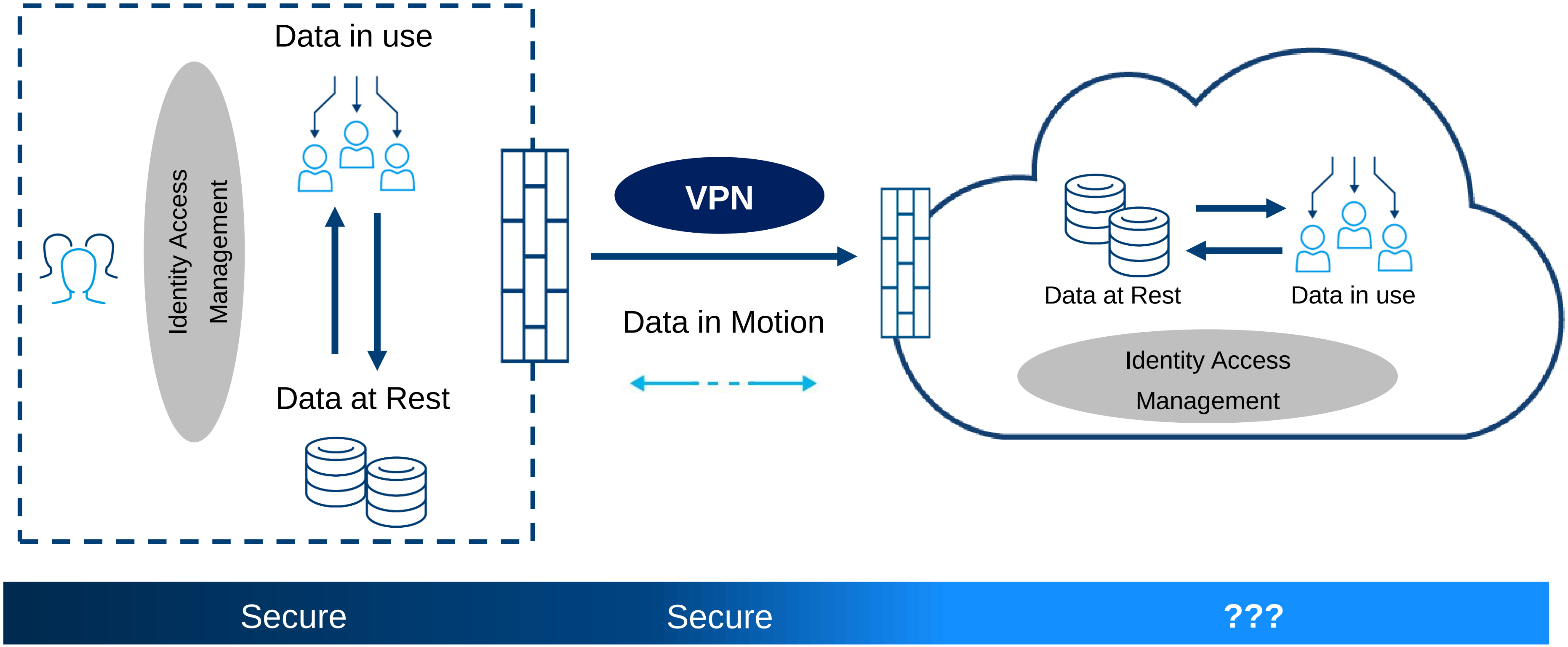
➢ **Major market players are, e.g. carriers and public network operators, with serious implementation plans**

► **Technology & Product-Fit for R&S**

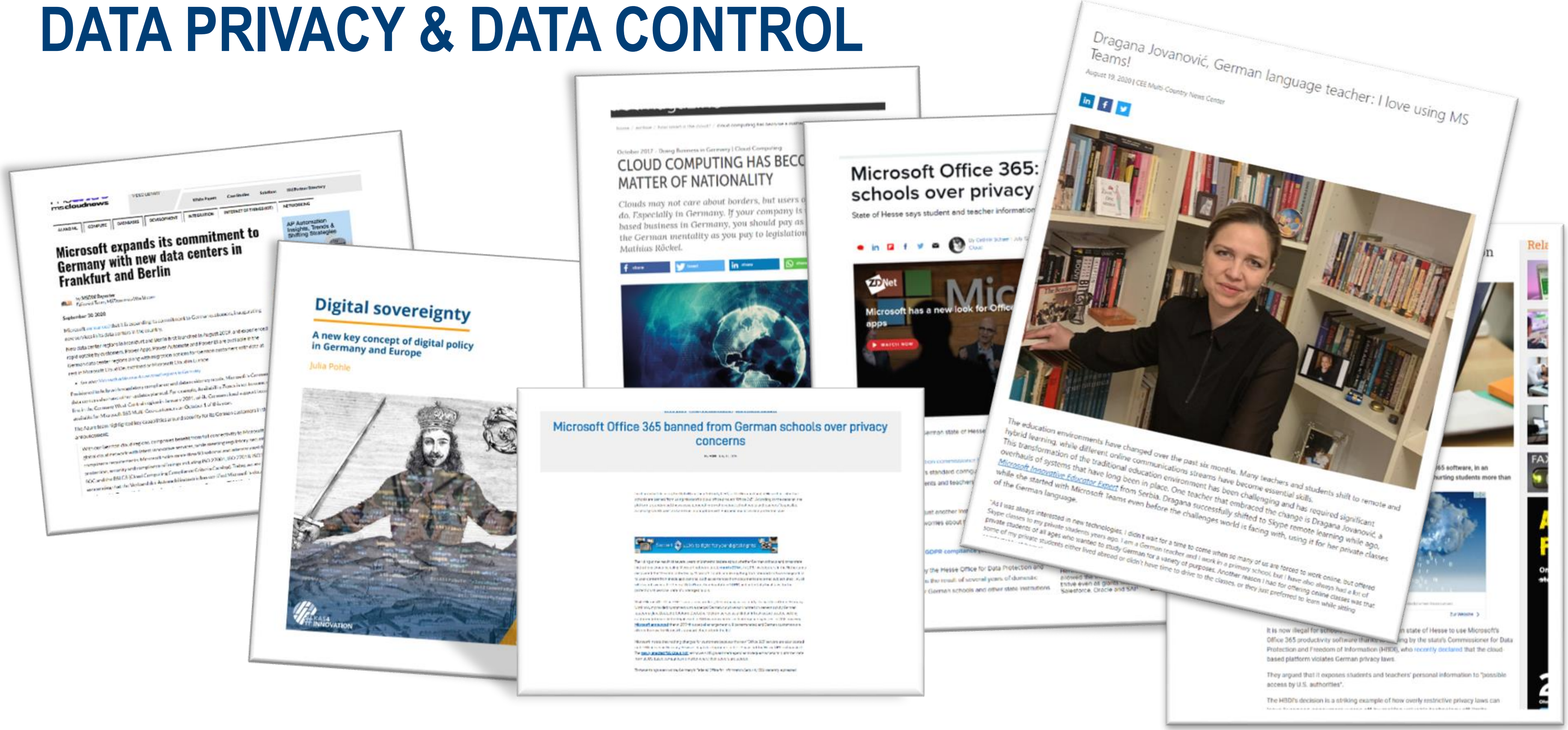
- QKD is a "natural" complement to network encryptors
- Technologies used connect seamlessly to RSCS portfolio & know-how (exception quantum optical part)
- R&S is perfectly positioned as a trustworthy German crypto & communication technology provider

DATA ENCYPTION IN THE CLOUD

COMMON SECURITY SOLUTIONS



DATA PRIVACY & DATA CONTROL



mscloudnews

Microsoft expands its commitment to Germany with new data centers in Frankfurt and Berlin

September 30 2020

Digital sovereignty

A new key concept of digital policy in Germany and Europe

Julia Pohle

October 2017 – Doing Business in Germany | Cloud Computing

CLOUD COMPUTING HAS BECO MATTER OF NATIONALITY

Clouds may not care about borders, but users d do. Especially in Germany. If your company is based business in Germany, you should pay as the German mentality as you pay to legislation Mathias Röckel.

Microsoft Office 365: schools over privacy

State of Hesse says student and teacher information

Microsoft has a new look for Office apps

Microsoft Office 365 banned from German schools over privacy concerns

Dragana Jovanović, German language teacher: I love using MS Teams!

August 19, 2020 | CEE Multi-Country News Center

The education environments have changed over the past six months. Many teachers and students shift to remote and hybrid learning, while different online communications streams have become essential skills. This transformation of the traditional education environment has been challenging and has required significant overhauls of systems that have long been in place. One teacher that embraced the change is Dragana Jovanović, a Microsoft Innovative Educator Expert from Serbia. Dragana successfully shifted to Skype remote learning while ago, while she started with Microsoft Teams even before the challenges world is facing with, using it for her private classes of the German language.

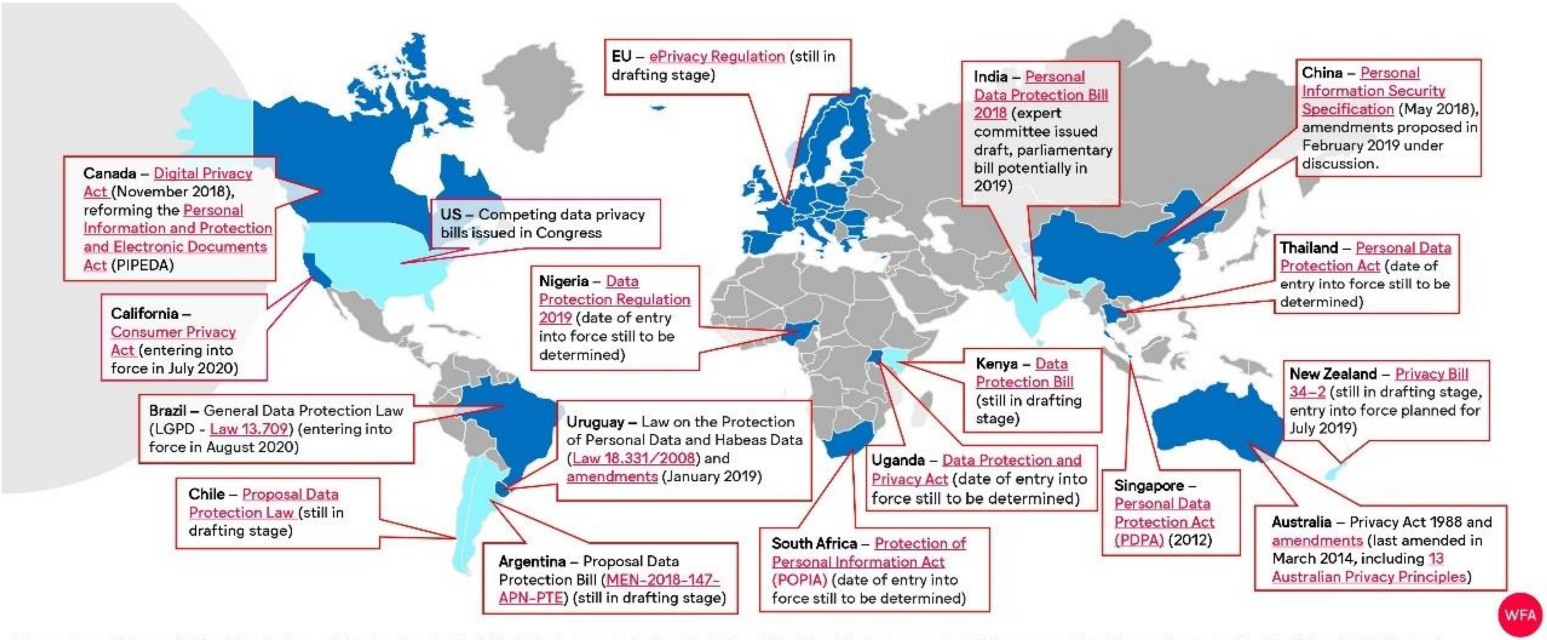
"As I was always interested in new technologies, I didn't wait for a time to come when so many of us are forced to work online, but offered Skype classes to my private students years ago. I am a German teacher and I work in a primary school, but I have also always had a lot of private students of all ages who wanted to study German for a variety of purposes. Another reason I had for offering online classes was that some of my private students either lived abroad or didn't have time to drive to the classes, or they just preferred to learn while sitting

It is now illegal for schoo n state of Hesse to use Microsoft's Office 365 productivity software thanks ng by the state's Commissioner for Data Protection and Freedom of Information (HBDI), who recently declared that the cloud based platform violates German privacy laws.

They argued that it exposes students and teachers' personal information to "possible access by U.S. authorities".

The HBDI's decision is a striking example of how overly restrictive privacy laws can

INTERNATIONAL REGULATIONS



Canada – Digital Privacy Act (November 2018), reforming the Personal Information and Protection and Electronic Documents Act (PIPEDA)

California – Consumer Privacy Act (entering into force in July 2020)

US – Competing data privacy bills issued in Congress

EU – ePrivacy Regulation (still in drafting stage)

India – Personal Data Protection Bill 2018 (expert committee issued draft, parliamentary bill potentially in 2019)

China – Personal Information Security Specification (May 2018), amendments proposed in February 2019 under discussion.

Thailand – Personal Data Protection Act (date of entry into force still to be determined)

Nigeria – Data Protection Regulation 2019 (date of entry into force still to be determined)

Kenya – Data Protection Bill (still in drafting stage)

New Zealand – Privacy Bill 34–2 (still in drafting stage, entry into force planned for July 2019)

Brazil – General Data Protection Law (LGPD - Law 13.709) (entering into force in August 2020)

Uruguay – Law on the Protection of Personal Data and Habeas Data (Law 18.331/2008) and amendments (January 2019)

Uganda – Data Protection and Privacy Act (date of entry into force still to be determined)

Singapore – Personal Data Protection Act (PDPA) (2012)

Chile – Proposal Data Protection Law (still in drafting stage)

Argentina – Proposal Data Protection Bill (MEN-2018-147-APN-PTE) (still in drafting stage)

South Africa – Protection of Personal Information Act (POPIA) (date of entry into force still to be determined)

Australia – Privacy Act 1988 and amendments (last amended in March 2014, including 13 Australian Privacy Principles)

* Focus only on certain key markets for global advertisers – this is not an exhaustive list of all legislative developments in all countries in the world. For information about any country which is not represented on this map, please contact Max Schmidt (m.schmidt@wfanet.org)

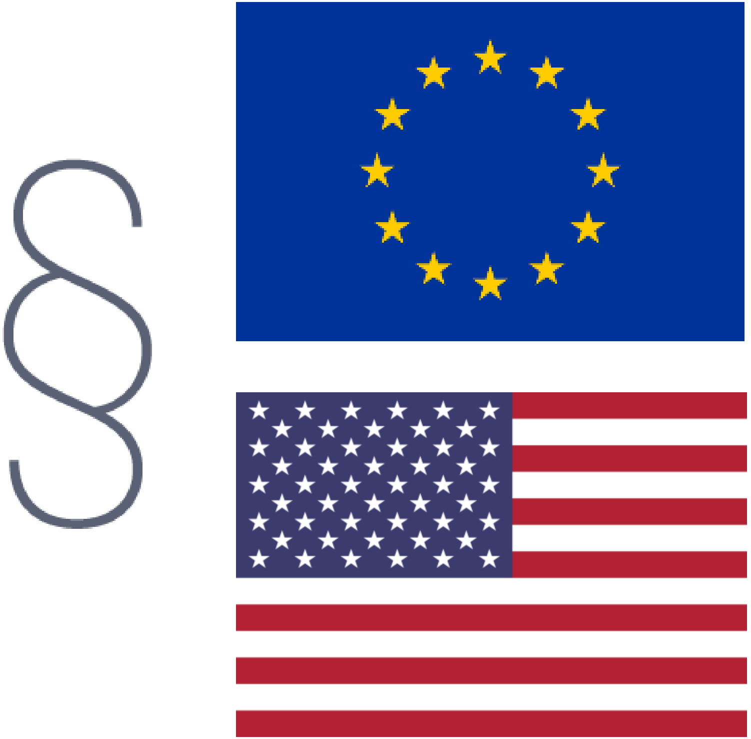
Source: https://wfanet.org/knowledge/item/GDPR-the-emergence-of-a-global-standard-on-privacy

PRIVACY SHIELD & SCHREMS II

- In July 2020 the European Court of Justice declared that the **EU–US Privacy Shield framework** is not valid

- Privacy Shield never did provide adequate protections to EU citizens on government snooping
  ➔ **Cloud Act**

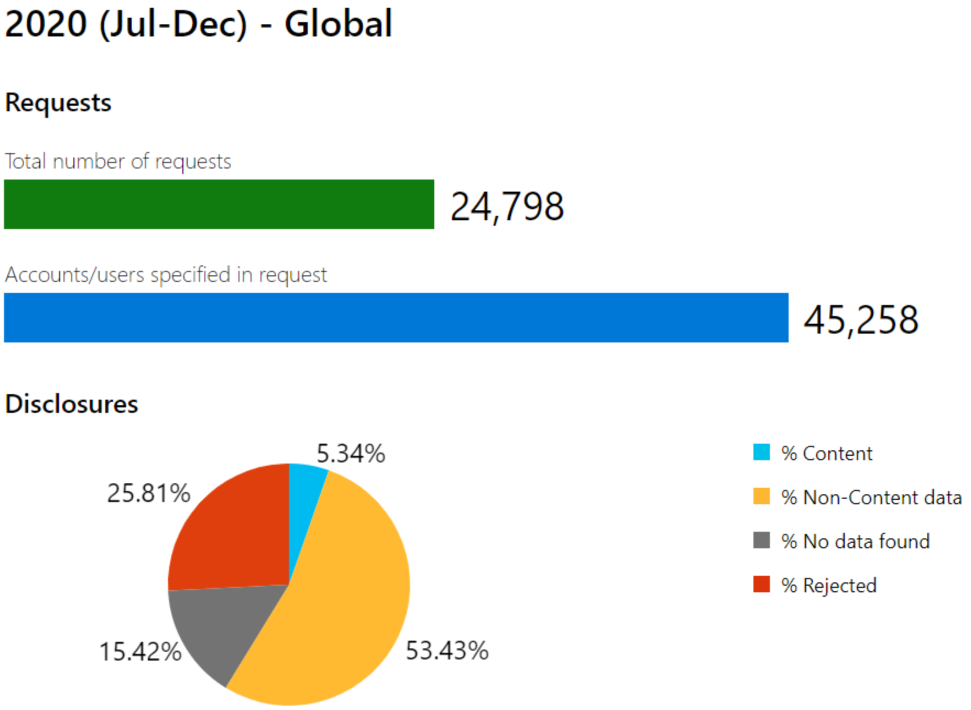
- Court declared that, "transfers on the basis of this legal framework are illegal“ for European companies and organizations -> **no GDPR compliance**



CLOUD ACT

> The CLOUD Act primarily … allow federal law enforcement to compel U.S.-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the U.S. or on foreign soil.

NUMBER OF LAW ENFORCEMENT REQUESTS TO ACCESS CUSTOMER DATA IN MICROSOFT 365 WORLDWIDE



2020 (Jul-Dec) - Global

Requests

Total number of requests

24,798

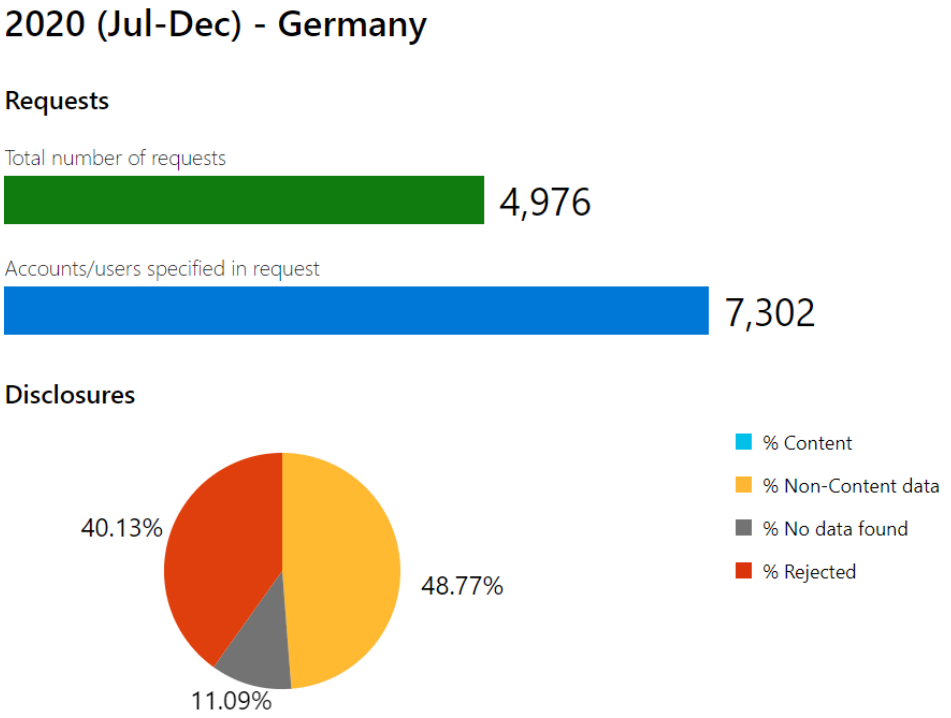
Accounts/users specified in request

45,258

Disclosures

Source: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report?culture=de-de&country=DE (16.07.2021)

NUMBER OF LAW ENFORCEMENT REQUESTS TO ACCESS CUSTOMER DATA IN MICROSOFT 365 GERMANY



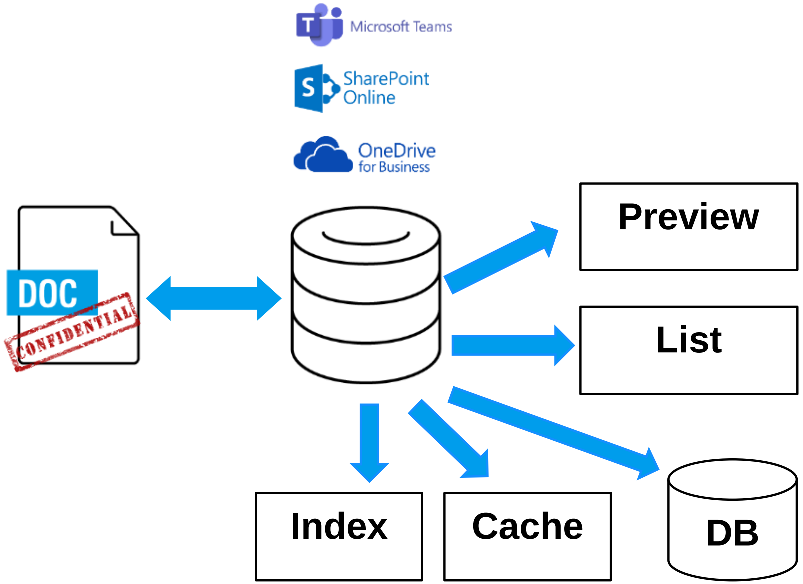
Source: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report?culture=de-de&country=DE (16.07.2021)

CHALLENGES

- Cloud solutions like Teams and SharePoint Online scan all documents immediately while being uploaded:
  - Full text search (index)
  - Previews etc.

- Confidential content is automatically distributed on the cloud platform

- Would an encryption before the upload help?
  - Encrypted data can’t be processed
  - No usual processes & workflows
  - No full text search



Regulated data from the user's perspective

USERS WANT TO FOCUS ON WORKFLOW AND NOT ON DATA PROTECTION

Please no further steps for my work!

For data exchange with external parties I know my own ways.

- ► Compliance rules
- ► Rules for document classification
- ► National and international regulations for data
- ► Restrictions for cloud platforms and restrictions on data exchange

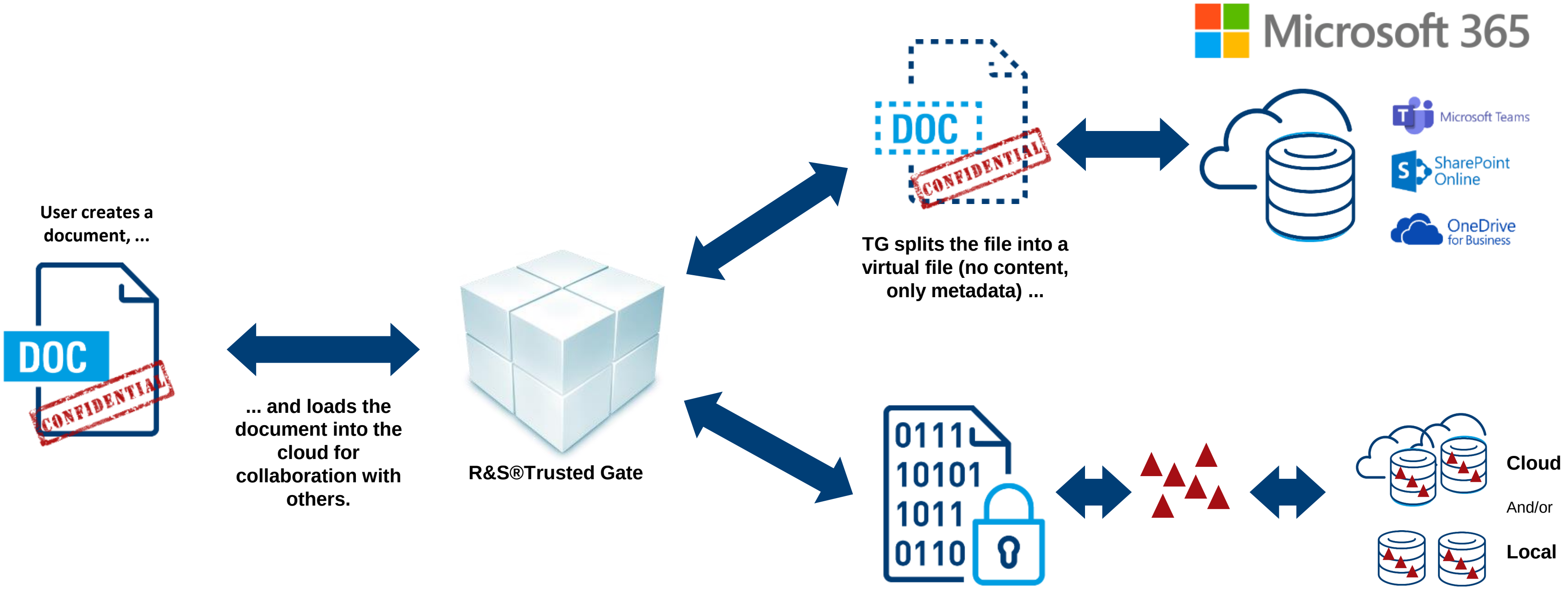
How should I classify this document?

Is this now confidential or does it contain personal data?

R&S®Trusted Gate

TRUSTED GATE

THE BASIC PRINCIPLE OF R&S®TRUSTED GATE



User creates a document, ...

... and loads the document into the cloud for collaboration with others.

R&S®Trusted Gate

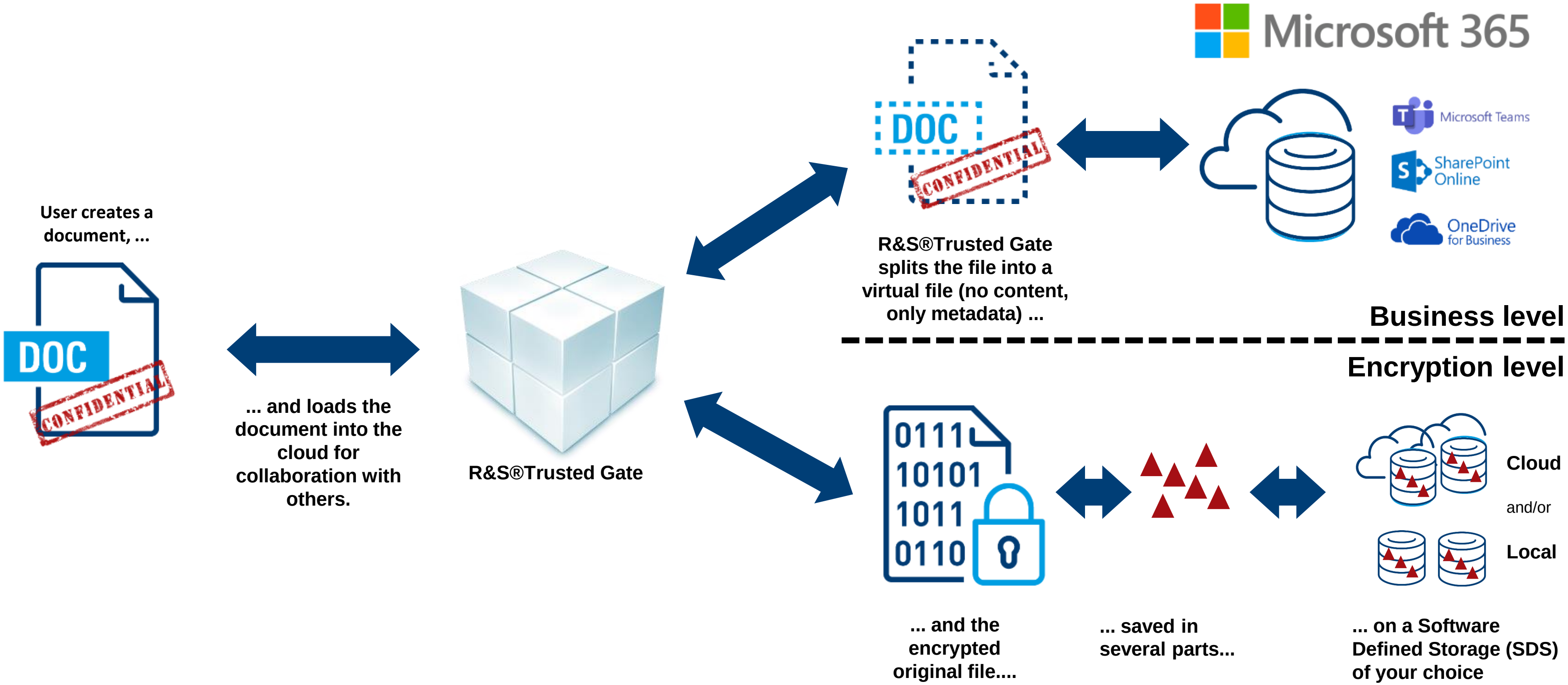
TG splits the file into a virtual file (no content, only metadata) ...

... and the encrypted original file....

... saved in several parts...

... on a Software Defined Storage (SDS) of your choice

THE BASIC PRINCIPLE OF R&S®TRUSTED GATE



User creates a document, ...

... and loads the document into the cloud for collaboration with others.

R&S®Trusted Gate

R&S®Trusted Gate splits the file into a virtual file (no content, only metadata) ...

Business level

Encryption level

... and the encrypted original file....

... saved in several parts...

... on a Software Defined Storage (SDS) of your choice

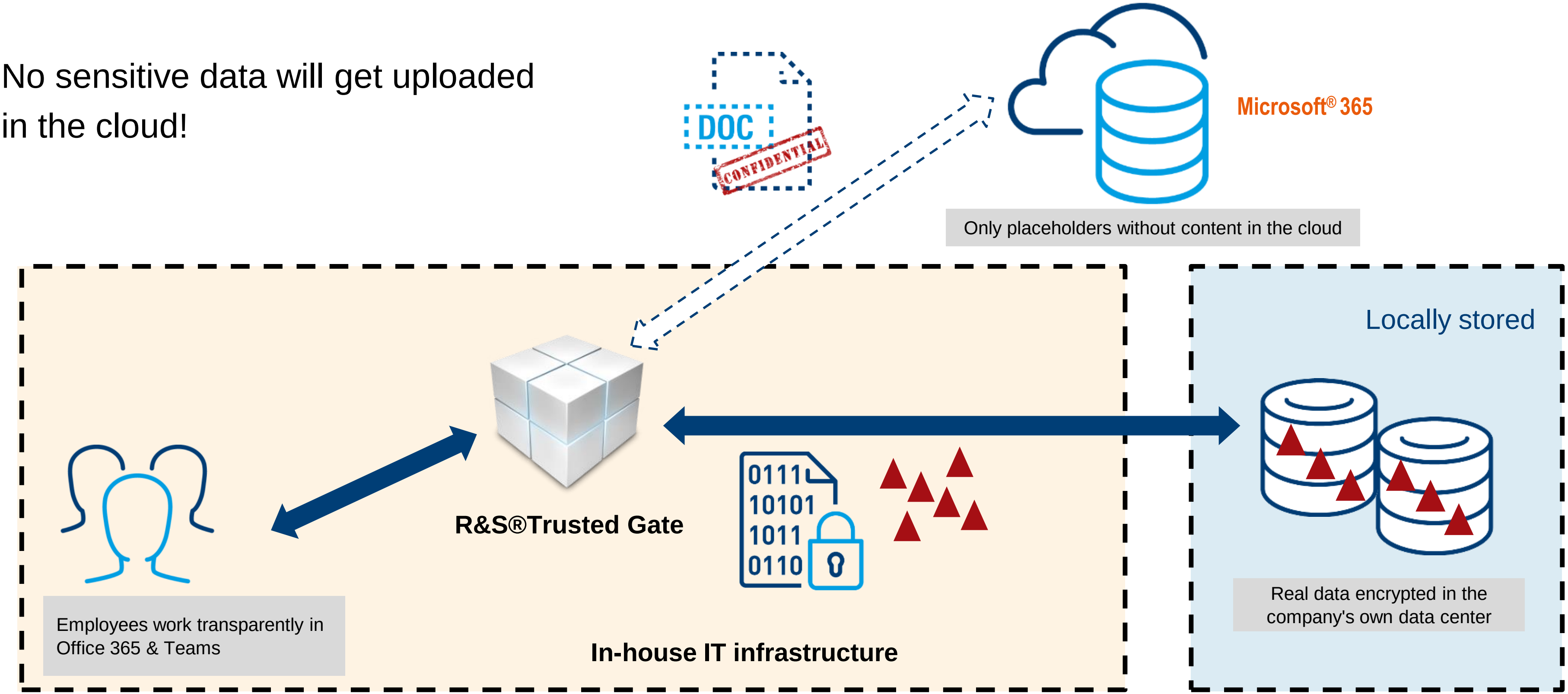
Cloud

and/or

Local

COMPANY FULLY CONTROLS DATA IN THE CLOUD

No sensitive data will get uploaded in the cloud!



Only placeholders without content in the cloud

Employees work transparently in Office 365 & Teams

Real data encrypted in the company's own data center

R&S®Trusted Gate Solutions

MICROSOFT 365 – TRANSPARENT ENCRYPTION

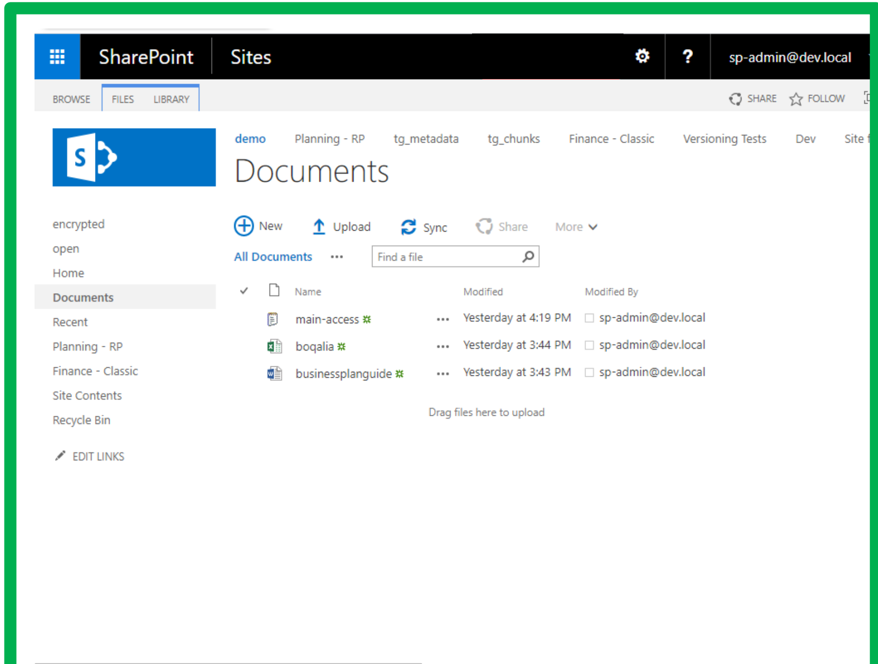
SCENARIO MICROSOFT TEAMS

„We do want to reorganize our way to work together in our company. Collaboration platform of our choice is Microsoft Teams. But ist complexity and deep cloud integration worries us when it comes to regulations like the GDPR.

How can we control our data in TEAMS?“

R&S®Trusted Gate Use Cases

SECURE COLLABORATION TRANSPARENTLY ENCRYPTED

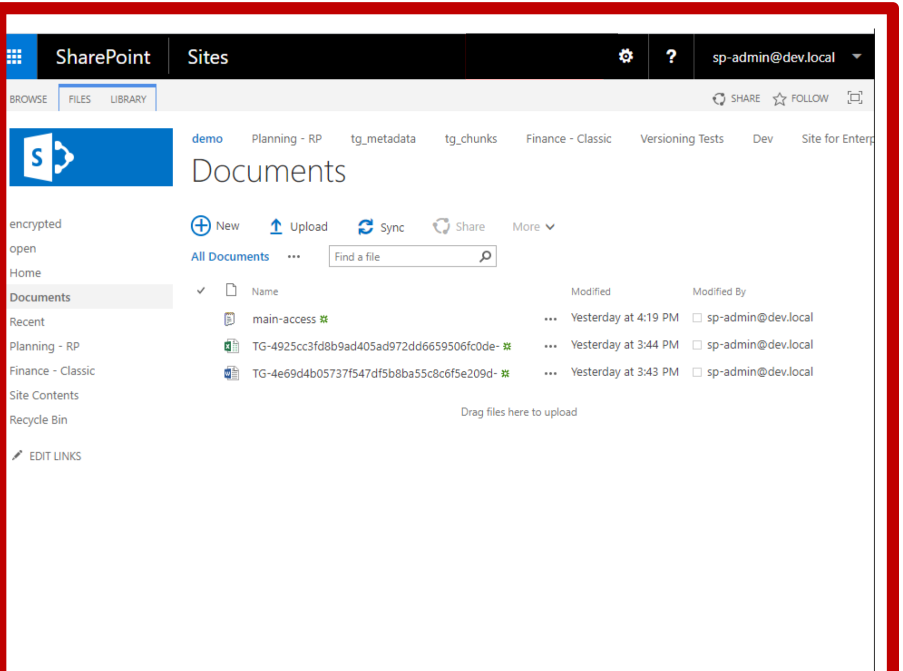


Documents

✓	Name		Modified	Modified By
	main-access	•••	Yesterday at 4:19 PM	□ sp-admin@dev.local
	boqalia	•••	Yesterday at 3:44 PM	□ sp-admin@dev.local
	businessplanguide	•••	Yesterday at 3:43 PM	□ sp-admin@dev.local

- No additional steps for users, they can keep all existing workflows

Adam – the worker



Documents

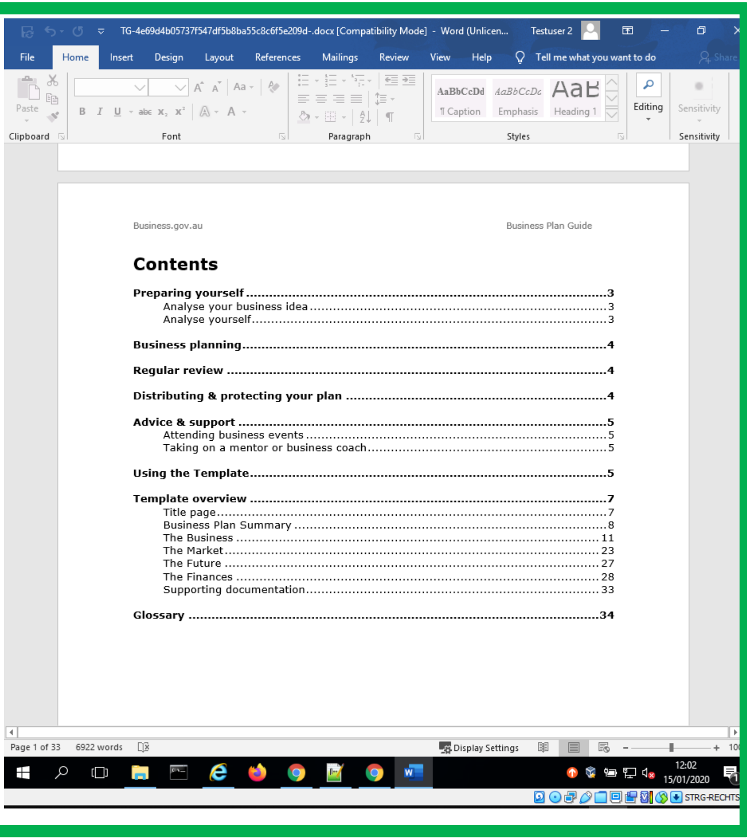
✓	Name		Modified	Modified By
	main-access	•••	Yesterday at 4:19 PM	□ sp-admin@dev.local
	TG-4925cc3fd8b9ad405ad972dd6659506fc0de-	•••	Yesterday at 3:44 PM	□ sp-admin@dev.local
	TG-4e69d4b05737f547df5b8ba55c8c6f5e209d-	•••	Yesterday at 3:43 PM	□ sp-admin@dev.local

Donald – the hacker

R&S®Trusted Gate is directly integrated into the Office 365.

R&S®Trusted Gate Use Cases

SECURE COLLABORATION TRANSPARENTLY ENCRYPTED



Business.gov.au Business Plan Guide

Contents

Preparing yourself 3
- Analyse your business idea 3
- Analyse yourself 3

Business planning 4

Regular review 4

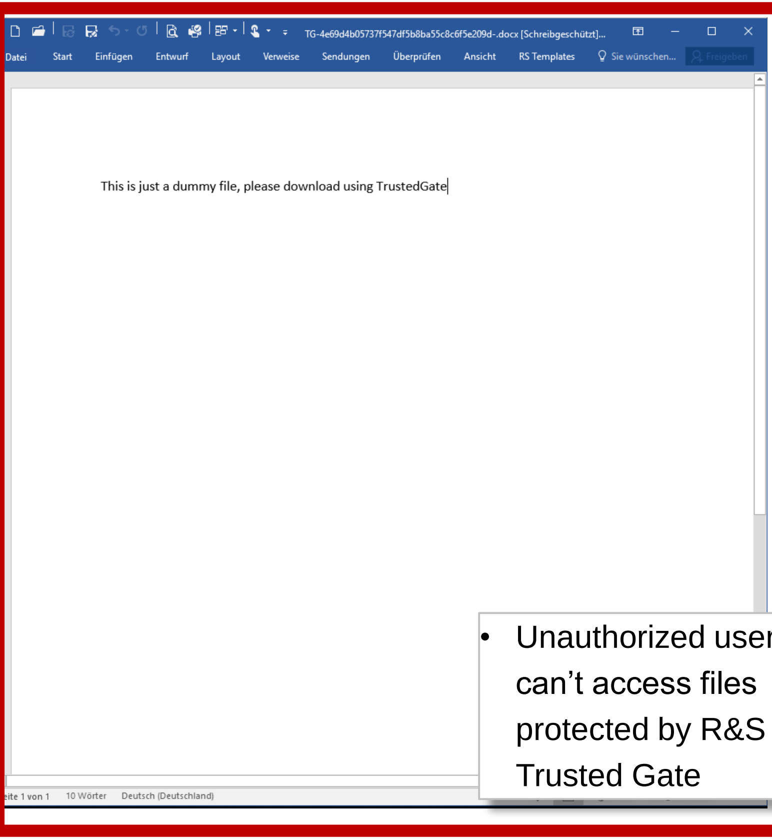
Distributing & protecting your plan 4

Advice & support 5
- Attending business events 5
- Taking on a mentor or business coach 5

Using the Template 5

Template overview 7
- Title page 7
- Business Plan Summary 8
- The Business 11
- The Market 23
- The Future 27
- The Finances 28
- Supporting documentation 33

Glossary 34

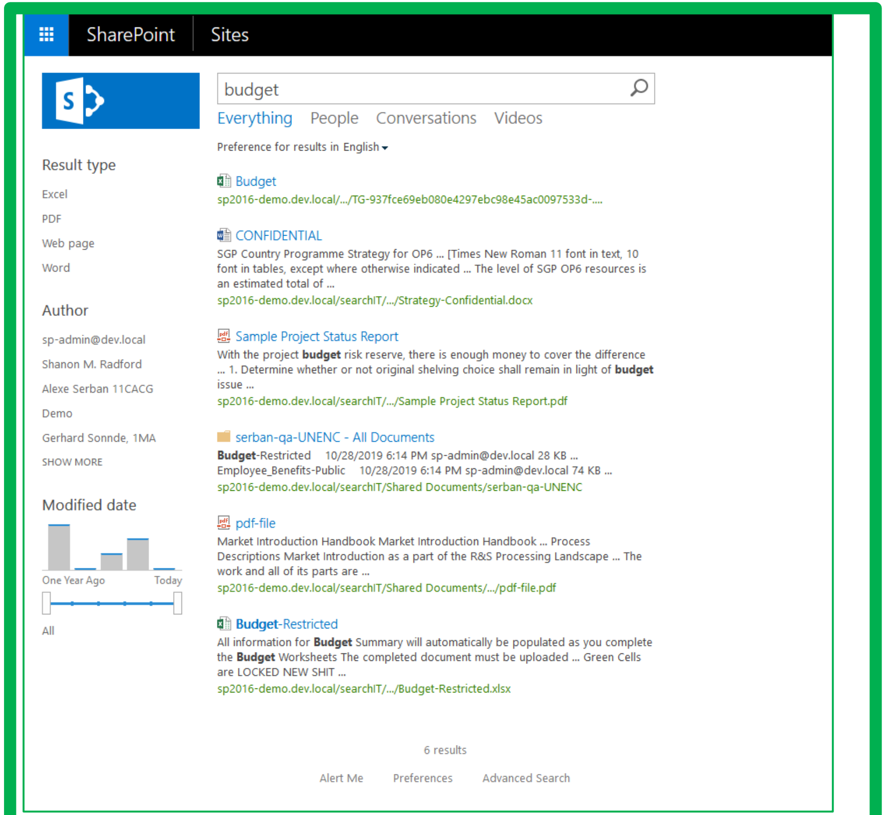


This is just a dummy file, please download using TrustedGate

- Unauthorized users can’t access files protected by R&S Trusted Gate

R&S®Trusted Gate Anwendungsszenarien

ENTERPRISE SEARCH



Budget
sp2016-demo.dev.local/.../TG-937fce69eb080e4297ebc98e45ac0097533d-....

CONFIDENTIAL
SGP Country Programme Strategy for OP6 ... [Times New Roman 11 font in text, 10 font in tables, except where otherwise indicated ... The level of SGP OP6 resources is an estimated total of ...
sp2016-demo.dev.local/searchIT/.../Strategy-Confidential.docx

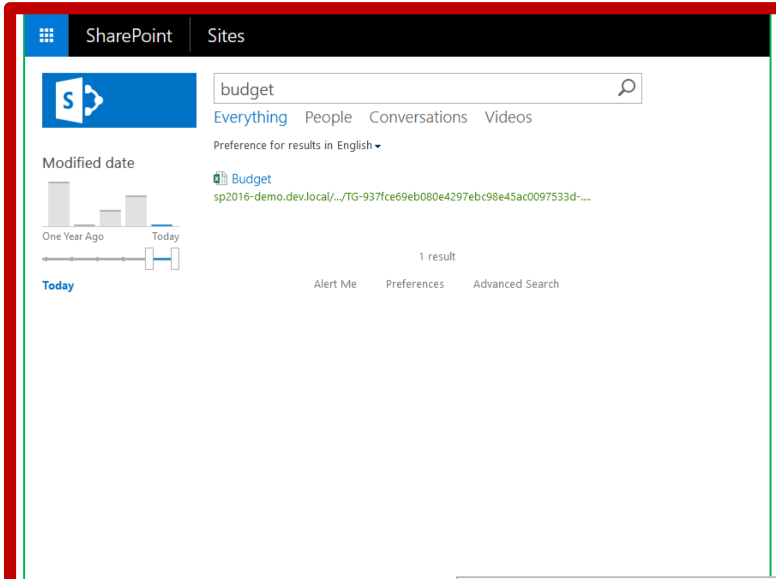
Sample Project Status Report
With the project **budget** risk reserve, there is enough money to cover the difference ... 1. Determine whether or not original shelving choice shall remain in light of **budget** issue ...
sp2016-demo.dev.local/searchIT/.../Sample Project Status Report.pdf

serban-qa-UNENC - All Documents
Budget-Restricted 10/28/2019 6:14 PM sp-admin@dev.local 28 KB ...
Employee_Benefits-Public 10/28/2019 6:14 PM sp-admin@dev.local 74 KB ...
sp2016-demo.dev.local/searchIT/Shared Documents/serban-qa-UNENC

pdf-file
Market Introduction Handbook Market Introduction Handbook ... Process Descriptions Market Introduction as a part of the R&S Processing Landscape ... The work and all of its parts are ...
sp2016-demo.dev.local/searchIT/Shared Documents/.../pdf-file.pdf

Budget-Restricted
All information for **Budget** Summary will automatically be populated as you complete the **Budget** Worksheets The completed document must be uploaded ... Green Cells are LOCKED NEW SHIT ...
sp2016-demo.dev.local/searchIT/.../Budget-Restricted.xlsx

6 results



Budget
sp2016-demo.dev.local/.../TG-937fce69eb080e4297ebc98e45ac0097533d-....

1 result

- Unauthorized users can’t get any Search results which are protected by R&S Trusted Gate

Rohde & Schwarz

R&S®Trusted Gate

TRUSTED GATE PRODUCT PORTFOLIO

R&S®Trusted Gate

PRODUCT PORTFOLIO

Secure Collaboration

Azure Marketplace Solutions

Cloud solution for secure working in AZURE.

Solution for Teams

Seamless integration for safe and transparent working in Microsoft® Teams™.

Solution for MS 365

Seamless integration for safe and transparent working in Microsoft® Office 365™ applications.

Solution for SharePoint

Securely encrypt documents in Microsoft® SharePoint™ and integrate them into existing workflows.

On-premises Solutions

High security solutions on-premises and hybrid.

Secure Data Exchange

Secure Data Exchange

Data room at the highest security level.

Data Diode

Secure data transmission between differently classified security domains.

Mail Control

Prevents the loss of confidential information via e-mail.

Mobile Access

Secure access to confidential content via mobile devices.

Secure Infrastructure

Pseudonymization

Working anonymously in the cloud.

EaaS – Encryption as a Service

Use SOAP/Rest APIs to enable internal applications with high security cryptography.

Infrastructure Optimization

Optimize existing infrastructures for multi tenants or multi security domains.

Solution for OneDrive™

Secure usage of OneDrive for Business with transparent data encryption.

Secure Glocalization

Keep you export controlled data inside national boundaries while collaborate globally.

THANK YOU!

ROHDE & SCHWARZ

Make ideas real

COMPANY RESTRICTED