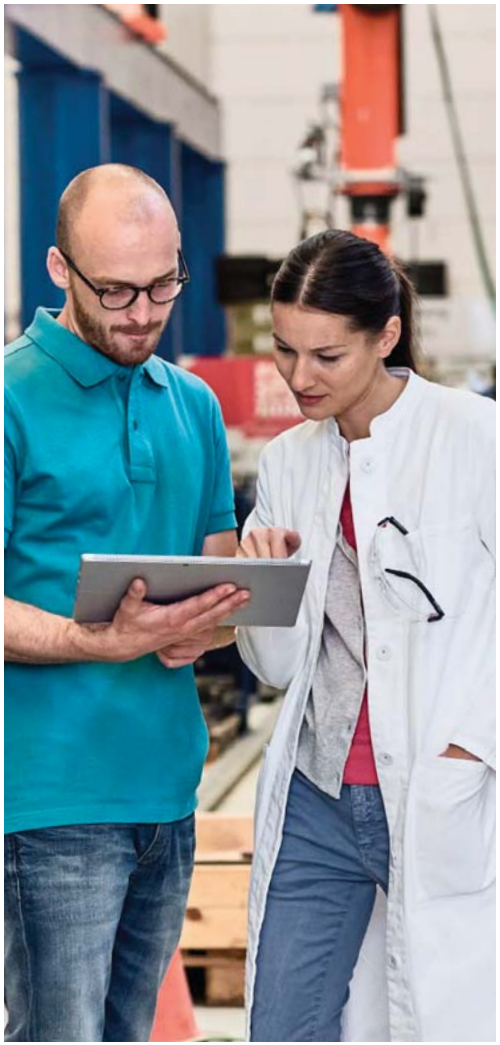
KEEPING THE CLOUD OF THINGS SECURE

HOW DEUTSCHE TELEKOM PROTECTS CUSTOMER DATA

LIFE IS FOR SHARING.

CONTENTS



1. THE CLOUD OF THINGS – IT ALL STARTS WITH ACCESS

1.1 M2M, IOT, THE CLOUD AND SECURITY

The Internet of Things opens up a wealth of opportunities for companies and helps them to prepare for the future: Preventive maintenance saves staffing costs and prevents expensive machinery downtime; automation of processes speeds up mechanical workflows and reduces the number of errors; and sensor data can be used to develop new business models.

With the Cloud of Things, Deutsche Telekom offers the perfect management platform for customers to network and monitor machines and devices, locate vehicles, or track the route and status of containers on screen. Sensor data is read in from the gateway, transmitted to the cloud platform in encrypted form, where it is processed and visualized. The customer designates which device will access their data.

1.2 THE CLOUD OF THINGS – SECURITY TAKES TOP PRIORITY

Despite these precautions, many companies have concerns about whether their data is safe in the cloud. Sensitive company data and business secrets have to be protected from unauthorized access; the protection of customer data has to be guaranteed. These are requirements that Deutsche Telekom takes very seriously, which is why security takes top priority when it comes to the Cloud of Things. Security is ensured by means of an extensive list of measures: All data is stored on servers in high-security data centers in Germany and is subject to Germany's strict data protection laws. Encryption is used to ensure a secure transport of data from the sensors. The network infrastructure, interfaces and IT systems through which the data travels uses standardized procedures and protection concepts to ensure data privacy and security.

Device Management
The Device Management aspect of the Cloud of Things provides an overview of all connected devices, their current operating status and the flow of data. This means that no updates are forgotten and security loopholes are avoided. Device management also helps with the detection of anomalies or attacks (intrusion detection), and automatically informs the administrator in the event of security breaches.

Remote maintenance of devices from the Cloud of Things
The Cloud of Things makes it possible for IoT devices to be maintained remotely, therefore keeping all components – including firmware and operating systems – up to date. This also eliminates potential security risks, which could arise as new methods of attack are developed. In addition, remote maintenance allows the user to update hard-to-reach machines – and protect them against possible dangers – without great input in terms of labor, time or funds.

2. SECURITY AND DATA PRIVACY AT DEUTSCHE TELEKOM

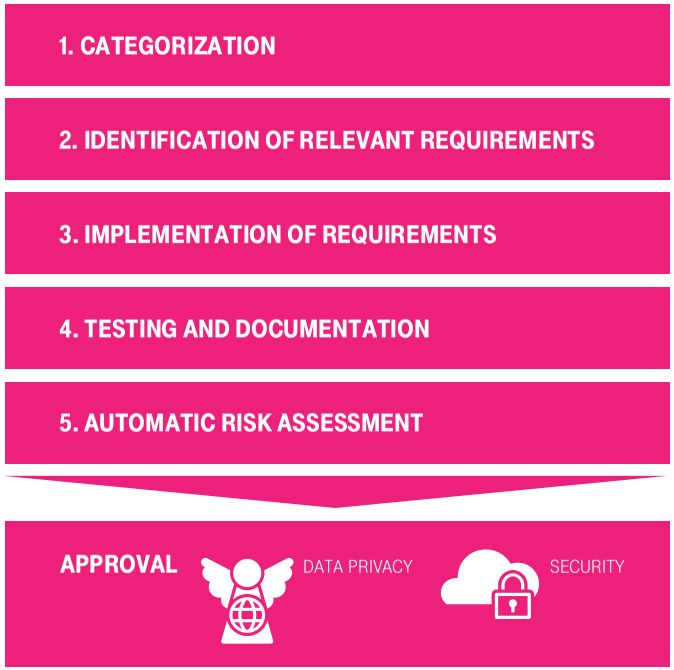
Two departments of Deutsche Telekom are dedicated solely to customer security: Group IT Security (SEC) and Group Privacy (GPR). SEC is responsible for technical security: It sets an appropriate security level and implements it using suitable measures. GPR determines the Group's strategic alignment in terms of data privacy and defines the requirements from a legal, technical and organizational perspective. It also represents the Group in all data privacy matters, both internally and externally. Deutsche Telekom's data privacy management is certified in accordance with IDW PS 980.

2.1 SECURE PROCESSES USING THE PSA METHOD

The German Federal Office for Information Security (BSI) has developed a list of measures that companies can use to ensure the security of applications, networks, IT systems and infrastructures. Based on this – and on the requirements of the European regulatory authorities regarding risk management for data privacy within companies – Deutsche Telekom has established a standard process for all of its products: The Privacy and Security Assessment ("PSA" for short).

The PSA method ensures the integration of security and data privacy into product and system development, and is applied upon each release of the Cloud of Things. This standardized Deutsche Telekom procedure includes consulting, testing and documentation, as well as risk assessment and approval.

A project's relevance in terms of data privacy and security is determined at the start of the process by means of a questionnaire. The categorization (A, B, C) is based on characteristics such as processing of particularly sensitive data, the complexity of the platforms and systems, or strategic and financial significance. The extent of consulting and support provided by Data Privacy and Data Security increases with the criticality and complexity of a project. The Cloud of Things has been categorized as "A", and therefore must meet the highest requirements.



An overview of the PSA procedure

"Our customers, shareholders, regulatory authorities and the general public rightly expect that we handle the data entrusted to us by our business partners, customers and employees with the appropriate care. We make every effort not just to satisfy these expectations, but to inspire yet more trust in our dependability. Data protection and information security are for us more than just a responsibility; we consider them a concern of particular importance to us. You can depend on that.

Dr. Claus-Dieter Ulmer,
Global Data Privacy Officer at Deutsche Telekom

THE AUDIT COMPANY

"As part of ISO 27001 certification of Deutsche Telekom's centralized security management, the PSA procedure was presented as one of the service processes provided by Group IT Security. The procedure was rated positively in the certification process as a useful, sensible way of prioritizing the processing of development projects from a data privacy and security perspective."

Peter Rothfeld and Ingo Vasen, external auditors from DQS GmbH,
Deutsche Gesellschaft zur Zertifizierung von Managementsystemen

2.2 STANDARDIZED SECURITY AND DATA PRIVACY CONCEPT

The PSA procedure involves a standardized security and data privacy concept (SDSK) comprising six modules:

- System description
- Data privacy information
- Authorization concept
- Lists of requirements
- Plan of measures
- System categorization

2.3 SECURE DATA CENTERS

Access to the physical infrastructure of a data center – or even the hardware – would provide an attacker with a good starting point for committing data espionage or manipulating services. An attacker could, for example, export and copy data via input/output interfaces or USB ports, import malicious codes, or disconnect services. As such, safeguarding the infrastructure is an important aspect of basic IT protection. This also includes protection against unforeseen events, which could lead to loss of services.

Extensive building protection
Data centers hosting the Cloud of Things are fully shielded and top security measures protect data from unauthorized access. The grounds, buildings and rooms are protected against unauthorized entry and break-in, and can only be accessed by authorized personnel. Access is monitored and, depending on the security level, the persons that have access to certain rooms at certain times are stored. Protection against fire and lightning strike, as well as water and high voltage damage, also form part of the extensive infrastructure protection. In addition, the power supply is fail-safe and protected against fluctuations in voltage, over-voltage and under-voltage.

Cloud data centers and product development processes are certified in accordance with the international ISO/IEC 27001 standard. This certificate, which is reviewed in regular intervals, attests that the company meets the security standards in terms of security guidelines, security requirements and risks.

The "Zero Outage" principle
Deutsche Telekom's "Zero Outage" program was established in 2011 and is certified – by TÜV Rheinland. Even an hour of downtime in IT systems can be critical to business operations and can cost a six to seven-figure sum – not to mention the damage to the company's reputation. With twin-core data centers, the latest technologies and trained staff, Deutsche Telekom ensures maximum IT availability – up to 99 percent –, as well as rapid, competent and efficient troubleshooting in the event of an outage.

High-security servers in the data center

Honeypots
In parallel with this, Deutsche Telekom has installed what are known as "honeypots" as a core component of its early warning system. These are isolated server systems which are accessible from the Internet but which are not connected to Deutsche Telekom's real systems.

The honeypot systems are self-teaching: They record unknown attacks and analyze them. Deutsche Telekom's experts use these analyses to prevent harmful attacks to the company's real systems, and to inform customers whose computers may have become part of a botnet. The method has proven to be a success: The honeypots have so far not uncovered any vulnerabilities in Deutsche Telekom's systems from the Internet.

"Deutsche Telekom is way above the general standard with this consolidated documentation of data privacy and security aspects and the technical/organizational measures implemented. Based on our long-standing experience in auditing and certification, the SDSK is an extremely positive development."

Monika Wojtowicz, Project Manager in Data Privacy Certification for Cloud Services at TÜV Informationstechnik GmbH

3. SECURITY IN THE CLOUD OF THINGS

In addition to the Group-wide security strategies in place at Deutsche Telekom, there are special measures taken to protect the IoT platform “Cloud of Things” against potential risks.

3.1 IT SYSTEMS

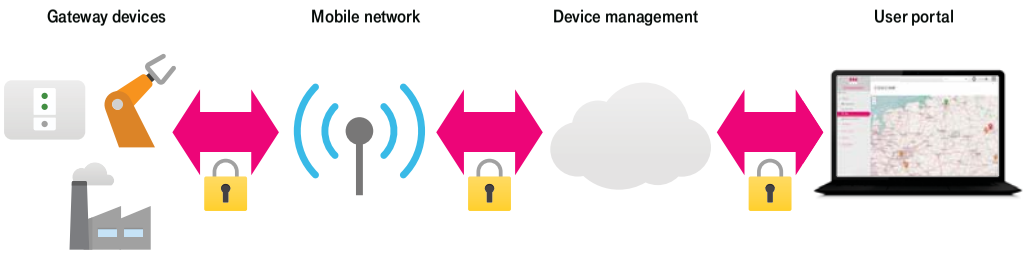
The kernels and software components used in Deutsche Telekom’s IT systems are subject to the highest requirements in terms of the maintenance of software versions and protection against viruses and malware. They can only be administered from the internal network and via virtual private networking (VPN), and are not accessible from the Internet. All data is stored in encrypted form.

Constant maintenance and monitoring
All components, such as operating systems, databases and application servers, are actively managed and subject to constant monitoring. Administration rights for the IT systems are awarded on an individual basis.

Overload protection
The IT systems for the Cloud of Things are protected against overload: The platform is protected against attempts to block services or knock the system off balance by flooding it with requests (DDoS attacks).

Approval of IT systems
Before every release, independent experts check the IT systems to ensure that the latest software versions and patches have been installed. As part of this inspection, they use penetration tests to simulate attacks, using a potential hacker’s procedure to attempt to get into the systems.

SECURE TRANSFER TO THE CLOUD OF THINGS



3.2 SECURITY ON THE INTERNET

A potential target for cyber attacks are the network connections between the customer’s browser and the Cloud of Things, as well as the radio link between the devices and the server platform. The infiltration of a radio or network link could then be the starting point for further espionage or attempts at sabotage: If an attacker has already uncovered usage and position data, recorded webcam videos or manipulated a smart home, their sabotage can destroy entire product families or a product or provider’s image – or they can blackmail manufacturers. Deutsche Telekom has an extensive list of measures to prevent this.

TLS authentication prior to each communication
Using a recognized and standardized authentication mechanism ensures that no third parties are able to intervene in the communication between an IoT device or a customer’s browser and the Cloud of Things. Prior to any communication via a network, the Cloud of Things proves its identity by means of a certificate. Certificates ensure that the communication partner is who they say they are – a source that is unable to provide an accepted certificate will never be trusted. This means that the authenticity of the platform is evidenced in the event of changes to the firmware or other exchange of data with the device.

The Cloud of Things uses the Transport Layer Security (TLS) protocol. In TLS, the communication partners check their authenticity by means of certificates and set up an encrypted connection. Data can then be shared securely: The connection is protected against attacks where the attacker assumes a fake identity, intervening between the sender and recipient and tapping into the data exchange (known as “man in the middle” attacks).

Encryption with AES
All data communication with the Cloud of Things is encrypted. This applies not only to access via the cockpit, but also to all communication between the IoT devices and the platform, in both directions. To this end, the Cloud of Things supports the secure Advanced Encryption Standard (AES) algorithm. This algorithm has been declared standard by the American National Institute of Standards and Technology (NIST). It is considered so secure that in the USA it is even authorized for use on official, top-secret documents. For customers whose devices do not support AES or whose security ratings do not require this, the Cloud of Things supports further encryption methods such as 3DES or Camellia.

Strong encryption ensures that no one can decrypt company or customer data if they obtain it by chance, illegally or through espionage, preventing them from using it for their own benefit, selling it or publishing it elsewhere. Making changes to data – “spoofing” – is also not possible: For example, an attacker cannot overwrite position data or virtually change the position of a truck, manipulate sensor data from a refrigerated container, or reproduce the signal from a garage door in a smart home (which would make it possible to open the door at any time).

Network separation
The core of the Cloud of Things is divided up into several sub-sections with different functions. The individual modules of these sub-sections work in their own cells, which, in turn, use independent network configurations with their own address zones. These virtual networks (VLANs) are isolated from one another in such a way that even if a hacker breaks into one VLAN, they will be unable to access another VLAN and expand the attack to other cells.

Firewalls
The Cloud of Things uses a multi-stage firewall concept to protect against access to the platform from insecure networks. All incoming requests must pass through the firewall: This applies to access from the website as well as to requests from IoT devices via the software interfaces of the Cloud of Things. Deutsche Telekom’s security experts check the firewalls regularly using penetration tests: This uncovers and resolves vulnerabilities and ensures that hackers have no chance of breaking through the firewalls.

3.3 ADDITIONAL MEASURES FOR INCREASED SECURITY

The interfaces in the Cloud of Things represent another target for attack. They are required for device management and data retention, and are also used to pass on alerts. Because they are accessible via the Internet, Deutsche Telekom has developed special concepts to protect them.

Multi-tenancy
The Cloud of Things has a multi-tenant structure: On the platform, different customers (tenants) have separate user areas and do not share administrator, data or address areas with other customers. It is not possible to view another tenant's customer data, user data or payload. For example, a logistics company will not have access to a competitor's customer or truck positioning data.

Separation of user data and payload
A second separating mechanism protects against espionage and manipulation of data: Within each tenant, customer and user data is managed and stored separately from payload. This means, for example, that in the Cloud of Things it is not possible to secretly send a database command when transmitting a GPS position (= payload), which would make it possible to obtain a customer's name (= customer data) and use it for other purposes.

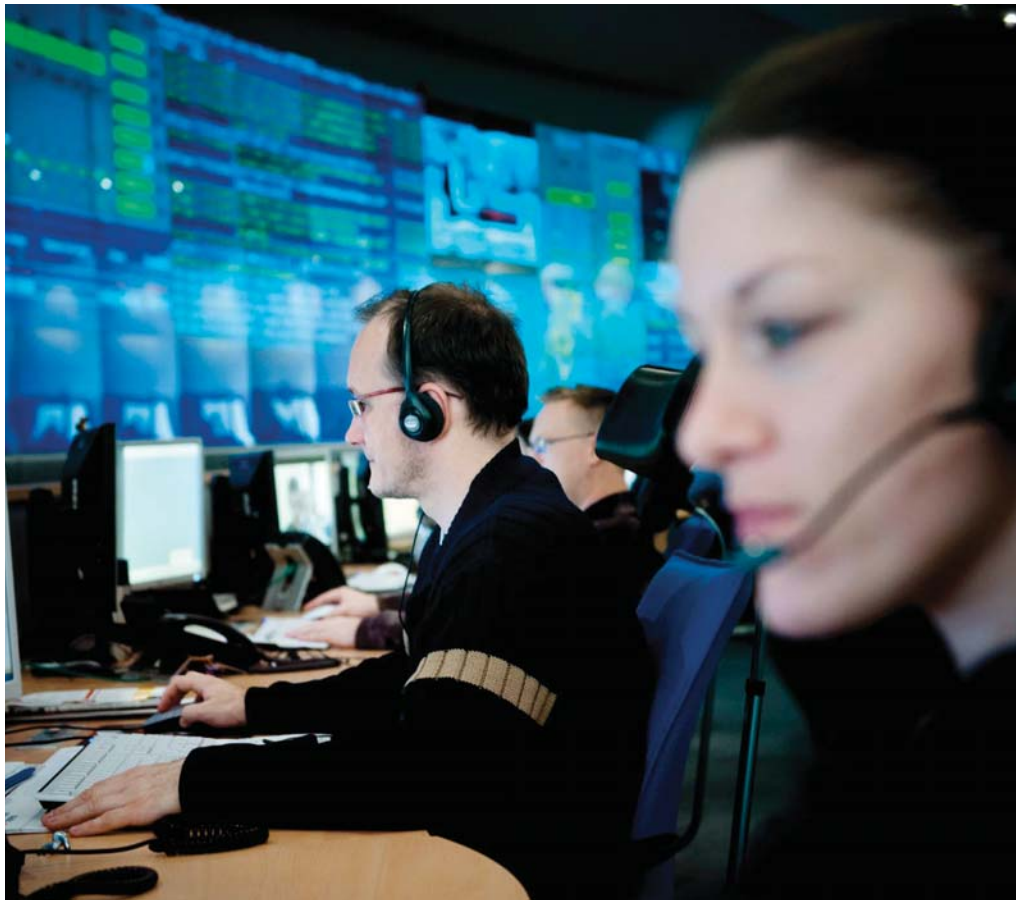
Authorization concept
Customers can define and authorize different user roles, such as administrator, standard user or business user, which are associated with different authorizations and privileges. This means that users can only view content for which they have been assigned rights in the user roles. The authorization concept defines who can generate, read, edit and delete data. Privileged rights are only assigned to roles, groups or people that are primarily entrusted with administration.

No built-in back doors
The Cloud of Things has properly defined and secured interfaces through the cockpit for manual users and through the software interfaces for devices. In addition, the Cloud of Things does not feature any additional ports or other built-in back doors, either for customers with their own interfaces or, for Deutsche Telekom, for maintenance and administration purposes. All requests have to be handled via the standard ports, and therefore through the same firewalls and security mechanisms. Even requests regarding administration and maintenance are not handled via dedicated interfaces that could be exploited by an attacker.

Approval by security experts before each releasee
In the event of new developments or changes, experts from Deutsche Telekom check whether the project meets all requirements in terms of technical security and data privacy. Approval by the security experts, who are organizationally and procedurally separated from the project and development teams, is mandatory before any release of the Cloud of Things – release without their approval is not possible.

Certification process for IoT devices
The experts at Deutsche Telekom check and certify all IoT devices that business partners may use with the Cloud of Things. This ensures that these devices meet the requirements in terms of technical security and data privacy. Customers that integrate their own devices and suppliers can request the relevant test criteria, or commission Deutsche Telekom to provide advice and carry out tests.

MAXIMUM SECURITY WITH THE CLOUD OF THINGS **SECURITY IN THE CLOUD OF THINGS**



Staff in the data center

4. TIPS FOR WORKING SECURELY IN THE INTERNET OF THINGS

Deutsche Telekom has an extensive list of measures to ensure the greatest possible security within the Cloud of Things. However, even the securest platform is useless if the customer's IT environment is not sufficiently protected. This checklist should help you to avoid typical mistakes when it comes to security.

4.1 PRINCIPLES AND GUIDELINES

Formal processes and guidelines are an important component: It helps to have a plan!

- **Conduct risk analyses:** Identify security risks, assess possible damage scenarios, take preventive measures
- **Define requirements:** Draw up requirements and checklists, define reference values and test criteria
- **Test for security:** Simulate targeted attacks using your own security staff, conduct penetration tests, draw up a list of tests, generate case studies, find testers, define a schedule for tests and audits, utilize test automation
- **Define acceptance strategies:** Define gates and schedules, appoint auditors, document results
- **Develop emergency plans:** Set out procedures for emergencies, provide for switch-off/shut-down of modules and systems, ensure operational continuity, create safety reserves, set out rules for communication and press relations

4.2 DEVICE SECURITY

Security measures must also be taken for the software and data on connected devices outside of the Cloud of Things – for example, on a computer used to access a web portal – to ensure that they are not used as a gateway for attacks. Deutsche Telekom recommends the following measures:

- **Load updates:** Close security loopholes in the operating system, update firmware, facilitate certificate updates
- **Change passwords:** Replace all standard passwords with your own passwords, use strong passwords, search for components installed in the background
- **Strengthen authorization:** Check authorization on the server (not on the client), facilitate password changes, enable changes to access details for other systems, provide for deletion of access data, use LDAP or comparable standard authorization backends
- **Use standard PKI:** Implement standardized Public Key Infrastructure (PKI) with certificate checks before any data communication, use TLS (where the client checks the server's certificate) or IPsec (both sides mutually check their certificates), use device-specific certificates, avoid sharing or joint use of certificates with other connected devices
- **Protect against malware:** Use anti-virus protection and keep it up to date
- **Encrypt memories:** Encrypt all local data carriers
- **Protect against overload:** Reject unauthorized data transfer at the point of entry, identify and react to overload situations caused by a flood of requests (DDoS), shut down systems in a controlled manner before unstable or unpredictable behavior arises
- **Provide rules for taking devices and services out of use:** Put devices and services out of use in the event of loss/theft/sale/at the end of the product's life, block access details, disable access, cancel certificates and licenses, uninstall software, delete memories, update entries in whitelists, shut devices and services down, remove hardware, ensure proper disposal

4.3 ENHANCING YOUR OWN SKILLS

It is recommended that you not only invest in technology and security concepts, but to also constantly expand your own skills and observe trends and necessary adjustments. Deutsche Telekom will be happy to help.

- **Briefing:** Brief employees, highlight dangers, define responsibilities, present techniques, provide materials
- **Training:** Provide training budget and training in concepts and techniques, procure advice and expertise, promote transfer of knowledge
- **Certification:** Have external checks conducted and processes certified, certify employees

5. SUMMARY

Without the Internet of Things there is no Industry 4.0 – and without security there is no Internet of Things. On the one hand, companies want to take advantage of the benefits of a cloud-based IoT platform in order to future-proof their business models. On the other hand, they want to be absolutely certain that company, customer and sensor data will not get into the wrong hands.

SECURITY AND DATA PRIVACY AT DEUTSCHE TELEKOM

With this in mind, Deutsche Telekom has given top priority to the security of its IoT platform "Cloud of Things". Throughout the Group, the Privacy and Security Assessment ensures the integration of data privacy and data security into system and product development. Data centers, from which the Cloud of Things is provided, are subject to the highest security standards: The high security data centers hosting the Cloud of Things are also armed against cyber attacks with an early warning system. The infrastructure benefits from extensive building protection and is safeguarded against unauthorized access, as well as against unforeseen events such as fire, flooding or power failure.

SECURITY CONCEPT FOR THE CLOUD OF THINGS

A special list of measures provides the Cloud of Things with additional protection. The operating system and software are immunized against viruses and malware. The systems are not connected to the Internet without protection, and all data is end-to-end encrypted. Bidirectional authentication precedes any network communication. IT systems are protected against DDoS attacks; databases and servers are actively managed. In addition, the platform is protected against unauthorized access by means of a multi-stage firewall.

The individual modules in the Cloud of Things work entirely independently of one another. This means that attacks on one module cannot affect other modules. Similarly, customer accounts are managed separately: Users are not able to access another user's area. Customer data, user data and payload is also stored independently. Users cannot be identified by their payload; data privacy is always guaranteed. With this comprehensive security package, Deutsche Telekom is paving the way for company applications in the Internet of Things.

GLOSSARY

3DES – Triple Data Encryption Standard: Precursor of AES

AES – Advanced Encryption Standard: Encryption method with an extremely high level of security

BSI – German Federal Office for Information Security

Camellia: A symmetrical block encryption method with similar parameters to AES, but with a different encryption algorithm

DDoS – Distributed Denial of Service: Unavailability of a service as a result of overload caused by a targeted attack on a server or another network component run by a large number of third-party systems

Firewall: A security gateway, comprising software and hardware, used to securely link up IP networks

IDS – Intrusion Detection System: System for detecting attacks on a computer system or network

M2M – machine-to-machine communication: Automated exchange of data between machines, devices, dispensers, vehicles and other terminals or with a central control center via the Internet, cellular networks and other access networks

Man-in-the-middle attacks: Intervention in communication between two partners by an attacker

Multi-tenancy: A computer system's ability to manage different tenants with independent data management, configuration and presentation

Penetration test: Simulated attempt to access your own IT system by using a method that might be used by a potential attacker

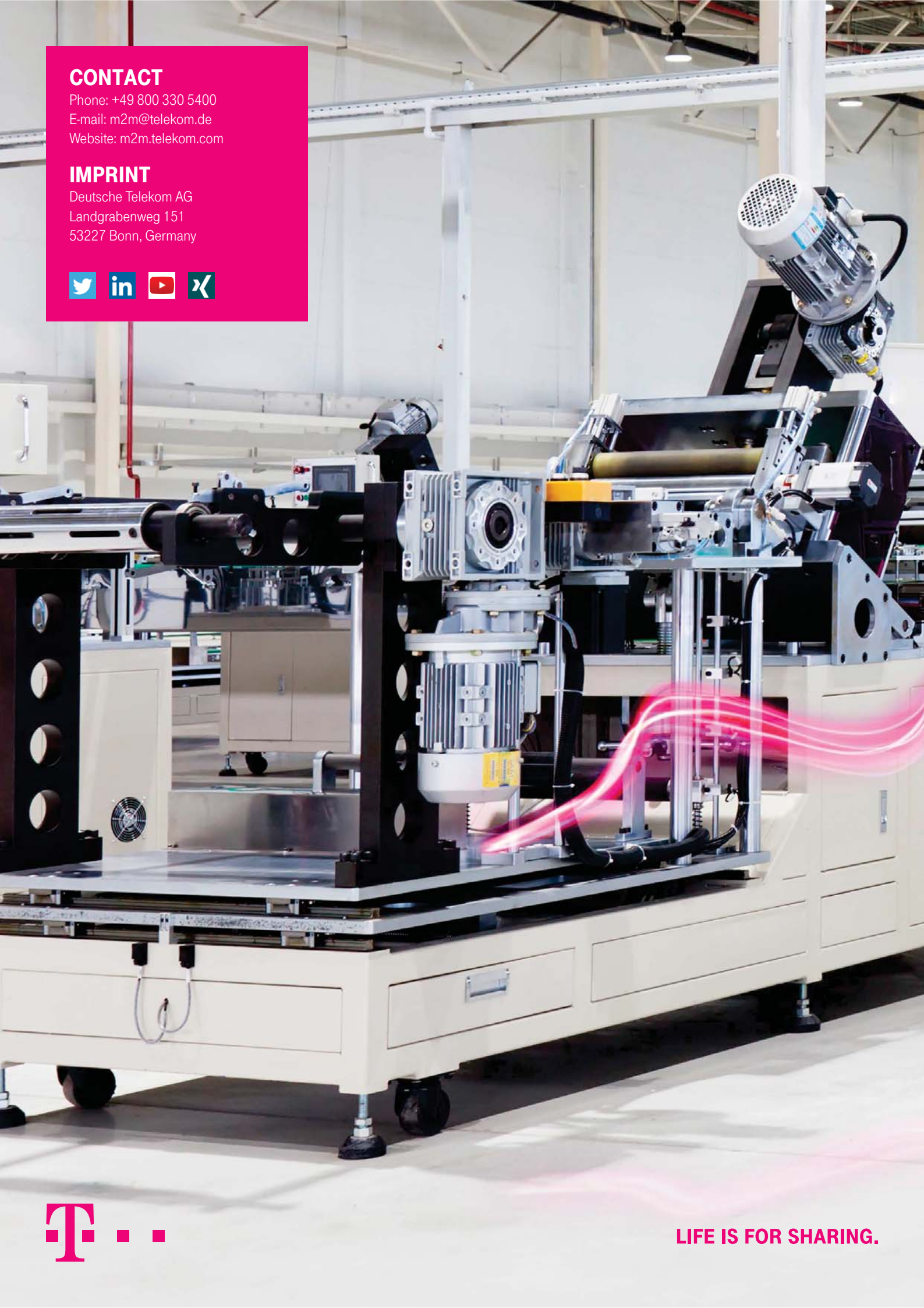
PKI – Public Key Infrastructure: A system for issuing, distributing and checking digital certificates for the purpose of authentication using a pair of public and private cryptography keys

PSA – Privacy and Security Assessment: Deutsche Telekom's standard process for ensuring security and data privacy in all of its products

Tenant: A group of computer system users that are isolated in terms of their data and have their own access authorizations

TLS – Transport Layer Security: Encryption protocol for data transmission, advancement of Secure Socket Layer (SSL)

VPN – Virtual Private Network: A closed communication network that uses a different communication network as a medium of transport, for example in the form of a VNP tunnel through the public Internet



CONTACT

Phone: +49 800 330 5400
E-mail: m2m@telekom.de
Website: m2m.telekom.com

IMPRINT

Deutsche Telekom AG
Landgrabenweg 151
53227 Bonn, Germany

LIFE IS FOR SHARING.