M2MGate – securely connected

The security architecture of our IoT platform

INSIDE M2M
SMART MACHINES

CONTENT

WHY SECURITY IS A PRIORITY IN THE IOT

In the connected world of Industrial IoT, the security of business-critical data and systems is paramount. As the operator of a fleet of devices, you face a fundamental challenge: every networked device can be a potential vulnerability, and at a time when cyberattacks are becoming more sophisticated and regulatory requirements are constantly increasing, you need a partner who not only understands your security requirements, but also implements them consistently. Protecting sensitive company data, adhering to data protection guidelines and defending against cyber threats are non-negotiable today.

Our goal is to develop the most secure products for our customers.

Following this principle, M2MGate was designed from the outset to meet the highest security standards while taking your specific compliance requirements into account. We see security not as an option, but as a fundamental principle.

M2MGate‘s holistic approach to security combines state-of-the-art encryption technologies, continuous security updates and comprehensive authentication mechanisms - providing you with a reliable shield for your Industrial IoT infrastructure.

1 THE SECURITY FRAMEWORK OF M2MGATE

The security of M2MGate is based on a comprehensive framework that is oriented towards the internationally recognized CIAAA protection goals. These protection goals form the foundation of our security architecture and are consistently taken into account throughout the entire software lifecycle - from the initial planning phase through to operation.

The five pillars of our security architecture

1. Confidentiality

We ensure that your sensitive data is only accessible to authorized users. We use modern encryption technologies and strict access controls to protect your company data from unauthorized access.

2. Integrity

The integrity of your data is our top priority. Our systems ensure that information cannot be changed unnoticed during transmission and storage.

3. Authenticity

Every communication and every data exchange is uniquely authenticated. This guarantees that all systems and users involved can be identified beyond doubt.

4. Authority

Granular authorization concepts enable precise control over who can access which resources. This prevents unauthorized access and ensures compliance with the “need-to-know” principle.

5. Availability

Your IoT infrastructure must function reliably. With redundant systems and proactive monitoring, we ensure that your services are available at all times.

These protection goals are manifested in M2MGate through specific technical implementations that are continuously reviewed and further developed. In this way, we ensure that your IoT infrastructure not only meets current security requirements, but is also equipped for future threat scenarios.

2 SAFETY MEASURES IN PRODUCT DEVELOPMENT

The development of M2MGate follows a comprehensive security concept that is anchored in all phases of product development. From initial planning to final deployment, we implement state-of-the-art security practices and technologies.

2.1 Planung

During the planning phase, we lay the foundations for a secure product. Through systematic **threat modeling**, we identify potential vulnerabilities and risks in advance. This involves an interdisciplinary team of development, product management and security experts to ensure a comprehensive perspective and to systematically categorize and evaluate threats. The results of the threat modelling flow directly into a **risk assessment**, which enables us to precisely estimate and prioritize the necessary security measures.

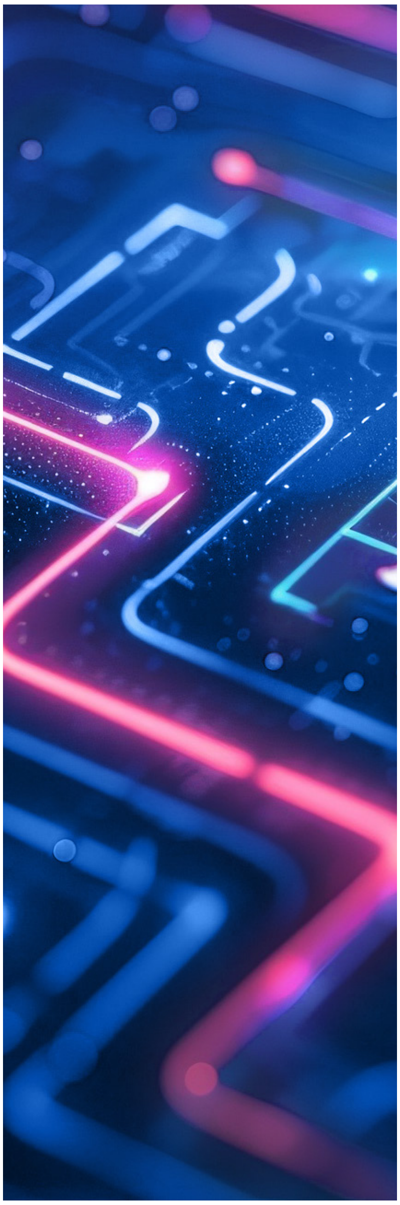
We consistently follow the **principle of least privilege** and a **zero-trust approach** in order to minimize the attack surface from the outset. This means that every module, every service and every user only receives the minimum necessary authorizations to fulfil their function. We specifically outsource standard components to **tested open source software**, allowing us to benefit from the security expertise of the community. These components are selected according to strict criteria, including checks for known vulnerabilities and active community support. Every step of the planning and risk analysis is carefully documented to ensure complete traceability and future audits.

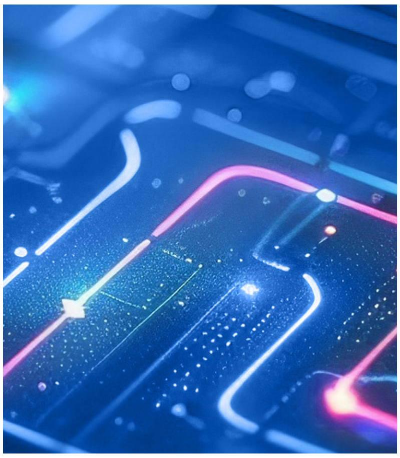
2.2 Development

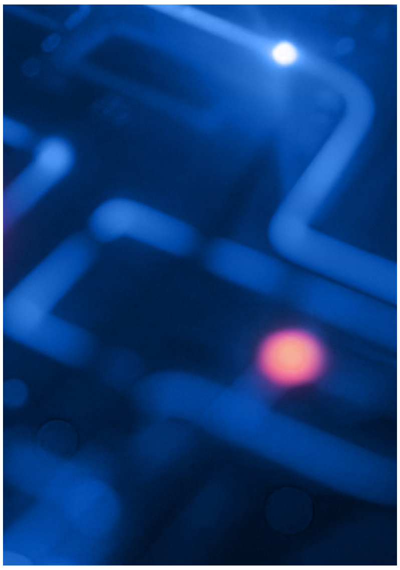
Our development processes are designed to ensure safety from the ground up:

- **Secure coding:** We rely on established secure coding practices and promote the regular exchange of knowledge within the development team. We continuously optimize our development practices through systematic reviews and retrospectives.

- **Workflow & code quality assurance:** New features are developed exclusively on separate branches. Every code change undergoes a strict review process before being integrated into the main development branches. For safety-critical components, we also use pair programming to ensure maximum code quality.







2.2.1 Source Code Management

Our source code is securely managed via GitLab, a robust DevOps platform that combines basic security features with efficient development support. Access to our source code is protected by a multi-level authorization concept:

- Role-based access control with fine-grained authorizations
- Mandatory **two-factor authentication** for all developers and secure authentication via SSH key

GitLab CE offers us important security advantages:

- **Basic safety functions:** Integrated access controls, protected branches and tags as well as secure user and group management.
- **Process automation:** Integrated CI/CD functionality, automated build and test pipelines and standardized merge request workflows.
- **Transparency and traceability:** Seamless logging of all changes, complete version history and comprehensive audit logs for project activities.

In addition, we ensure the integrity and quality of our source code through the following measures:

- **Strict branching strategies (e.g. Gitflow):** New features are developed exclusively on separate branches to avoid disruption to the main development branch and to ensure controlled integration. Every code change undergoes a review process before being integrated into the main development branches.
- **Comprehensive code reviews:** Every code change is reviewed by at least one other developer to identify errors and potential security vulnerabilities at an early stage. For security-critical components, we also use pair and mob programming to ensure maximum code quality.
- **Automated security scans in the CI/CD process:** Before merging, the code is automatically scanned for known vulnerabilities and compliance violations. This includes both static code analyses (SAST) and dependency checks (SCA) using SBOM analyses with Dependency Track.
- **Immutable infrastructure principles:** Our deployment pipelines ensure that code only enters the production environment via defined and secured paths and prevent manual changes that could pose potential security risks.
- **Training and awareness:** Our developers receive regular training in secure coding practices and are informed about the latest security threats and standards. The regular exchange of experiences within the development team is an integral part of our security culture.

These measures ensure that the source code of M2MGate is not only managed efficiently, but also continuously checked for the highest security standards.

2.2.2 Continuous review

Our development process includes systematic code revisions that cover both the application code and external dependencies. We pay particular attention to the continuous monitoring of our software supply chain through SBOM (Software Bill of Materials) analyses with Dependency Track. This powerful platform enables us to:

- **Real-time monitoring of vulnerabilities in all components used**
- **Automatic notifications of newly discovered vulnerabilities**
- **Precise risk assessment using CVSS scores**
- **Continuous license compliance checks**
- **Complete transparency of all software components and their dependencies**

2.3 Documentation

Comprehensive and up-to-date documentation is fundamental to the safety and maintainability of our product. Our central documentation system comprises various coordinated documentation levels:

Technical documentation: Detailed descriptions of all product modules, interface definitions and API specifications, as well as documentation of security measures and mechanisms

User documentation: Detailed installation and configuration instructions, as well as detailed descriptions of all (security) functions

System documentation of the cloud environments with infrastructure specifications, network architecture, backup and disaster recovery concepts, as well as monitoring and logging configurations

Audit and compliance documentation: logs of all manual security checks, as well as audit reports and their tracking, documentation of security incidents and their resolution

All documentation is versioned and regularly checked to ensure it is up to date. Access rights are assigned according to the need-to-know principle and checked continuously.

2.4 Deployment

Deployment is carried out via M2MGate Blueprint - an approach in which the provision of service configurations and orchestration is also fully controlled via CI/CD pipelines. All configuration changes are thus saved in the source code management system in a versioned form.

Regular audits and continuous SBOM checks ensure the highest security standards even after deployment.

These interlocking security measures ensure that M2MGate not only meets the highest security requirements at the time of delivery, but is also protected against new threats in the long term.

3 PRODUCT SAFETY: INTEGRATED PROTECTION MEASURES

To ensure the highest level of security, M2MGate implements a range of comprehensive protection measures built directly into the platform. From continuous connectivity to secure remote access, here's how our platform robustly protects your IoT infrastructure against modern cyber threats.

3.1 Always Online: Bidirectional communication

M2MGate establishes a permanent, bidirectional connection between your IoT devices and our servers. This "always-online" architecture not only enables real-time monitoring and control of your device fleet, but also forms the basis for comprehensive security functions. The continuous connection ensures that security updates are rolled out immediately, threats are detected instantly and necessary countermeasures can be initiated without delay. Efficient data transmission enables all relevant system and security parameters to be analyzed. For you, permanent connectivity means:

- **Immediate detection and response to security-relevant events**
- **Continuous monitoring of device statuses**
- **Immediate implementation of security measures**
- **Prompt distribution of security updates**
- **Effective prevention of security incidents through real-time monitoring**

3.2 Secure data connections

At M2MGate, the security of all data connections is our top priority. We implement state-of-the-art encryption and authentication mechanisms to provide comprehensive protection for your communications.

All device connections are authenticated via Mutual TLS (mTLS), in which both communication partners must prove their identity using digital certificates. A sophisticated certificate provisioning process ensures the secure initial setup and renewal of certificates. All service connections are also secured by mTLS and additional certificate pinning, which effectively prevents man-in-the-middle attacks.

3.2.1 Modern encryption standards

All communication channels are encrypted exclusively with the latest TLS versions 1.2 or 1.3. These proven encryption standards ensure that the connections meet the highest security requirements and at the same time offer optimum performance. These standards offer:

- **State-of-the-art encryption algorithms**
- **Perfect Forward Secrecy**
- **Protection against known attack vectors**
- **Optimized performance with maximum security**

3.2.2 Secure remote access

For remote access to your devices, M2MGate offers advanced VPN and stream functionalities that ensure a secure connection from anywhere. These features are specifically designed to combine security and ease of use to enable smooth remote maintenance and management.

- **Encrypted TCP tunnels for secure point-to-point connections**
- **Integrated support for common remote protocols (VNC, RDP, SSH)**
- **Gateway-based architecture for an additional layer of security**

This multi-layered security architecture ensures that your sensitive data is optimally protected at all times - both during transmission and when accessing your devices remotely.

3.3 Device certificate management

The secure management of device certificates is a central component of our security concept. M2MGate implements advanced certificate management that relies on both automation and the highest security standards. This ensures the integrity and availability of your IoT infrastructure and reduces manual administration efforts.

3.3.1 Automated certificate management

Our system handles the fully automatic renewal of all device certificates. This process ensures that devices always have valid, up-to-date certificates without the need for manual intervention. This minimizes risks and maximizes operational efficiency. This ensures:

- **Uninterrupted operation thanks to timely certificate renewal**
- **Minimization of human error through automation**
- **Continuous monitoring of certificate validity**

3.3.2 Secure key storage

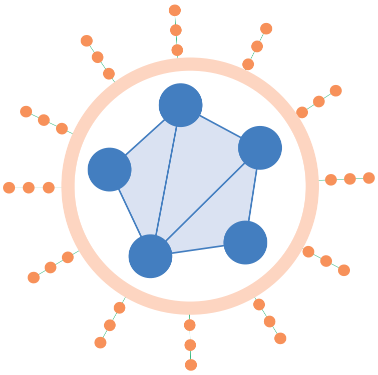
For maximum security, M2MGate supports the storage of cryptographic keys in dedicated security modules - provided this function is supported by the gateway hardware used. This integration with modern security hardware provides an additional layer of protection against unauthorized access and ensures the integrity of your cryptographic keys.

- **Integration with Hardware Security Modules (HSM) for enterprise-grade security**
- **Support of TPM 2.0 for additional hardware protection**
- **Secure key generation and storage**
- **Protection against unauthorized access to cryptographic material**

This combination of automated certificate management and the integration of secure hardware standards ensures that your device certificates are optimally protected. At the same time, smooth, uninterrupted operation of your infrastructure is guaranteed at all times.

3.4 Integrated firewall

M2MGate implements a stringent firewall concept that maximizes the security of your IoT devices through a "Zero Trust" architecture. We specifically eliminate potential attack surfaces, guarantee precise access control and ensure that all communication is secure and monitored.



3.4.1 Closed system architecture

A fundamental security principle of M2MGate is the complete absence of open, incoming ports on the devices. The closed system architecture reduces the attack surface to an absolute minimum and prevents attackers from establishing unauthorized access or carrying out network-based attacks. This means:

- **Minimal attack surface thanks to closed ports**
- **No direct access points for potential attackers**
- **Effective protection against port scanning and network-based attacks**
- **Reduction of the risk of unauthorized access**

3.4.2 Centrally controlled access control

All communication with the devices is handled exclusively via the secure M2MGate CascadeServer infrastructure. This architecture allows complete control over all access, combined with comprehensive logging and strict authentication measures. This architecture offers:

- **Centralized control of all access**
- **Complete logging of communication**
- **Granular access control**
- **Multi-level authentication**

Thanks to this strict access control and the closed system architecture, M2MGate guarantees optimally secure operation of your IoT infrastructure.

3.5 M2MGate Distribution Service: automatic security and firmware updates

In a constantly evolving threat landscape, the timely distribution of security and firmware updates is critical to maintaining a high level of security. With the M2MGate Distribution Service, we offer a powerful, automated solution for the secure and reliable management of updates - regardless of the size or complexity of your IoT device fleet.

3.5.1 Fully automatic update distribution

Security and firmware updates are distributed via a centrally controlled and fully automated process. We attach particular importance to the integrity of the updates, a smooth rollout and the traceability of all processes. This minimizes the risks for your IoT devices and ensures maximum operational reliability. Our distribution service ensures the seamless and automated distribution of updates:

- **Centrally controlled roll-out of security updates**
- **Automatic check of update integrity**
- **In the event of unexpected problems or compatibility issues during the update, the system can be automatically or manually reset to a previously functioning firmware version to minimize downtime.**
- **Every step of the update process, from distribution to successful installation or rollback, is logged in detail. This enables complete traceability for audits and analyses.**
- **Phased update deployment (staging): Updates can be rolled out to a small group of test devices first to identify potential issues in a controlled environment before a broad rollout. This minimizes the risk of malfunctions across the entire device fleet.**

3.5.2 Highly scalable architecture

To avoid downtime and enable reliable update distribution to large device fleets, the M2MGate Distribution Service is based on a highly scalable architecture. This has been specially designed to address thousands of devices simultaneously and minimize the impact on ongoing operations.

The Distribution Service infrastructure has been specifically designed to meet the requirements of large device fleets:

- **The architecture is designed for high connectivity and simultaneous processing of large update requests.**
- **M2MGate optimizes data transfer to avoid network congestion, especially in environments with limited bandwidth.**
- **Updates are designed to run in the background, minimizing disruption to regular device operation.**

This combination of fully automated management and a highly scalable infrastructure makes it possible to distribute security and firmware updates efficiently and reliably - regardless of how large or geographically distributed your device fleet is. This ensures that all devices are always up to date to minimize risks and maximize your operational security.

The M2MGate Distribution Service gives you the flexibility and security you need to meet the growing demands of the IoT security landscape.

3.6 User administration in the M2MGate portal

Effective and secure user management is fundamental to protecting your IoT infrastructure. In the M2MGate portal, we rely on Keycloak as a central identity and access management (IAM) solution to combine enterprise-grade security with user-friendly administration. With this powerful tool, we ensure that all users and authorizations can be managed reliably and in accordance with the highest security standards.

3.6.1 Keycloak as IAM solution

Keycloak offers a wide range of modern functions that centralize authentication and authorization and systematically minimize security risks. By using this open source technology, our users benefit from a flexible and constantly evolving management system that offers comprehensive security and administration options. Our use of Keycloak offers several decisive advantages:

- **Central authentication and authorization**
- **Comprehensive security functions such as brute force protection**
- **Multi-factor authentication**
- **Session management and token-based authentication**
- **High level of adaptability and expandability**
- **Open source transparency and active community**

3.6.2 Enterprise-Integration

To meet enterprise requirements, Keycloak supports seamless integration with Microsoft Entra ID (formerly Azure AD) and other existing enterprise identity providers. This makes user management not only more secure, but also seamlessly integrated into existing business processes. With Keycloak, we enable seamless integration with Microsoft Entra ID and Azure AD:

- **Federation with existing identity providers**
- **Single sign-on (SSO) across organizational boundaries**
- **Use of existing corporate identities**
- **Central management of user accounts**
- **Automatic deactivation when employees leave**
- **Enforcement of company-wide password policies**

3.6.3 Role-based access control

The fine-grained user and rights management is based on a role-based access control system (RBAC) implemented via Keycloak. This enables precise customization of user rights and ensures maximum security, while being flexible enough to be adapted to the specific requirements of your organization.

Our granular RBAC system, implemented via Keycloak, ensures maximum security through:

- **Precise definition of user rights and roles**
- **Principle of least privilege**
- **Flexible adaptation to organizational structures**
- **Grouping of authorizations by function**
- **Detailed audit logs of all accesses and changes**

This combination of the robust Keycloak platform, enterprise-grade identity management and fine-grained access control enables you to securely and efficiently manage all users and their authorizations in the M2MGate system. You retain full control over your system at all times, while your users benefit from simple and secure system operation.

3.7 Remote-Debugging

M2MGate offers advanced options for secure remote maintenance and troubleshooting that combine fast response times with maximum security. With our remote debugging solution, we not only enable efficient troubleshooting of technical problems, but also create the basis for proactive maintenance management - all without compromising the security of your systems.

3.7.1 Real-time diagnostics and troubleshooting

Reliable and secure error analysis in real time is essential for solving technical problems quickly and effectively. Our remote debugging functions make it possible to analyze device statuses in detail and carry out targeted diagnostics - without requiring physical access to the devices or on-site deployment. Our remote debugging functionality enables:

- **Immediate response to technical problems**

- **Secure real-time analysis of device statuses**

- **Targeted diagnostics without physical access**

3.7.2 Efficient fault management

By providing direct access to your devices, our remote debugging not only minimizes downtime, but also reduces the need for costly on-site interventions. This leads to a significant optimization of operational resilience while increasing efficiency. The possibility of direct device access offers decisive advantages:

- **Drastic reduction in system downtime**

- **Avoidance of costly on-site visits**

- **Rapid problem identification and resolution**

- **Proactive maintenance through early detection of potential problems**

- **Optimized mean time to repair (MTTR)**

All remote debugging activities are carried out via encrypted connections and are subject to strict access controls so that the security of your systems is never compromised.

3.8 Maximum availability of your IoT infrastructure

The availability of your IoT infrastructure is more than just an operational objective - it is a fundamental security aspect. An unavailable infrastructure can not only cause operational disruptions, but also open up significant security gaps. M2MGate therefore takes a multi-layered approach, combining intelligent network management, optimized data transmission and security strategies to create a reliably available platform.

3.8.1 Connection Bearer - Flexible network management

Stable access to the infrastructure is the basis for a highly available IoT solution. Our connection bearer ensures that your devices remain connected at all times - regardless of the stability of individual networks. Through intelligent connection management, we ensure seamless communication, even under difficult connection conditions. Our intelligent connection management ensures uninterrupted communication:

- **Multi-connectivity through parallel support of LTE, Ethernet and WiFi**
- **Automatic failover between different connection types**
- **Seamless switching between connections without data loss**

3.8.2 Ultra-fast and compact Object serialization

Data transmission poses a particular challenge for IoT applications, especially in resource-constrained environments or with limited bandwidth. Our specially optimized object serialization reduces latency, minimizes bandwidth requirements and ensures reliable transmission of your data - even under unfavorable network conditions. The optimized data transmission is specially tailored to IoT requirements:

- **Minimal latency times thanks to efficient serialization**
- **Reduced bandwidth requirements thanks to compact data formats**
- **Resource-saving implementation for edge devices**
- **Reliable transmission even with weak connections**
- **Integrated mechanisms for data consistency**

3.8.3 Availability as a security objective

At M2MGate, ensuring high availability is closely linked to security considerations. Uninterrupted operation enables continuous monitoring of the infrastructure and the prompt distribution of security and software updates. This keeps your IoT infrastructure not only functional, but also protected against potential threats. The high availability serves several security aspects:

- **Continuous monitoring of device security**
- **Prompt distribution of security updates**
- **Rapid response to security incidents**
- **Maintaining security functions even under difficult network conditions**

This multi-layered strategy to ensure availability makes M2MGate a robust and reliable platform for your business-critical IoT applications. We ensure that your infrastructure is not only operational at all times, but also meets the highest security requirements.

4 M2MGATE: OPERATIONAL RELIABILITY WITHOUT COMPROMISE

At INSIDE M2M, we attach great importance to offering our customers flexible options as to how they want to operate M2MGate.

If you choose to procure M2MGate through our INSIDE M2M hosted services, we ensure operational security through a multi-level, proactive approach. This covers all aspects of operations - from infrastructure in German data centers to continuous monitoring and risk response. Our goal is to provide you with an environment in which your IoT infrastructure is not only stable and highly available, but also uncompromisingly protected against current and future threats.

If you host M2MGate in your own infrastructure, INSIDE M2M will support you with comprehensive best practices and recommendations to ensure a high level of operational security.

In this document, we focus on the security measures and architecture that apply when INSIDE M2M hosts M2MGate.

4.1 German data centers according to ISO 27001

The choice of location and the architecture of the selected data centers form the basis for the security of your data and systems. M2MGate is operated exclusively in German data centers that are certified in accordance with the internationally recognized ISO 27001 standard. This strategic orientation guarantees the highest information security and data protection standards and at the same time meets the specific compliance requirements of our customers, who attach great importance to location loyalty and legal security.

4.1.1 Certified safety standards

ISO 27001 certification ensures that the data centers have implemented comprehensive and systematic information security measures. These include precisely specified processes that cover both physical and technical protection mechanisms to ensure data integrity and availability. The ISO 27001-certified data centers offer, among other things:

- **Comprehensive physical security measures**
- **Redundant infrastructure systems**
- **Strict access controls**
- **Continuous security monitoring**
- **Regular security audits**

4.1.2 Location Germany

Our decision to use only German data centers underlines our commitment to handling your data in a legally compliant and transparent manner. German data centers are subject to strict data protection regulations, which are supplemented by comprehensive European data protection laws (such as the GDPR). This makes Germany one of the most secure and legally compliant locations for data storage in the world. The German location guarantees:

- **Compliance with strict European and German data protection laws**
- **Legal certainty thanks to clear legal classification**
- **Transparent data storage and processing**
- **Protection against unauthorized access by third countries**
- **Short latency times for European customers**

This combination of certified security in the data centers and the German location forms the foundation for trustworthy and compliant operation of your IoT infrastructure. Our approach combines state-of-the-art security standards with the legal and technological advantages that a service operated in Germany offers.

4.2 M2MGate: Deployment and system updates

The secure provision and continuous updating of our systems is a core component of operational reliability. M2MGate relies on a multi-level, automated approach that provides seamless security and process control from development through deployment to quality assurance. This enables us to ensure operational stability and maximum security without compromising usability.

4.2.1 Container security

Our container infrastructure forms the basis for a flexible and scalable system architecture. In order to actively minimize security risks, we subject container images to continuous checks that focus on vulnerabilities, security and stability. With the help of modern tools and processes, we ensure that identified risks are remedied at an early stage. Our container infrastructure is subject to strict security controls:

- **Continuous scanning of all container images for vulnerabilities**
- **Automatic detection and assessment of CVEs (Common Vulnerabilities and Exposures)**
- **Proactive remediation of identified security issues**
- **Use of minimally privileged base images**
- **Regular updating of the container base**

4.2.2 Automated deployment

Secure and efficient deployment requires a transparent, automated process pipeline. M2MGate uses modern CI/CD pipelines that not only automate the entire deployment process, but also have important security checks built in at every stage to ensure consistency and security:

- **Fully automated build and deployment processes**
- **Integrated security tests in every pipeline**
- **Traceable versioning of all changes**
- **Automatic rollback mechanisms in the event of problems**
- **Continuous monitoring of the deployment status**

4.2.3 Operating system management

A stable and constantly updated operating system basis is essential for the security and reliability of a system. By using Linux Debian, our systems benefit from its robust security standards, efficiency and long-term support. By using Linux Debian, we ensure:

- **Regular, automated security updates**
- **Standardized update cycles**
- **Long-term stability and support**
- **Transparent security patches**
- **Efficient patch management**

4.2.4 Quality assurance through staging

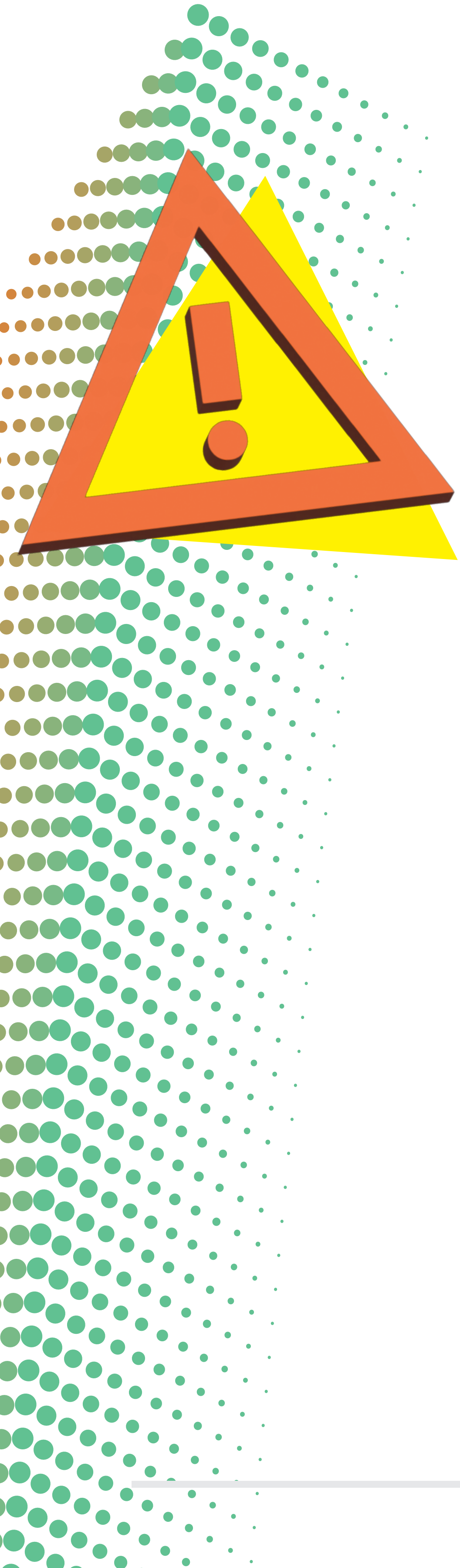
Our multi-stage staging system is an essential part of the deployment process. It provides an isolated environment in which updates can be comprehensively tested before they are transferred to the productive systems. This minimizes downtime risks and ensures a seamless introduction of changes. Our multi-stage staging system enables:

- **Comprehensive testing of all updates before going live**
- **Early detection of potential problems**
- **Validation of security updates in a realistic environment**
- **Verification of system compatibility**
- **Minimization of downtime risks in productive operation**

These interlocking processes ensure secure and reliable operation while keeping all system components up to date. By combining automated technologies with proactive security analytics and detailed testing, we offer a robust technical foundation, technical excellence and the highest level of security.

4.3 Proactive monitoring and logging

M2MGate implements a comprehensive monitoring system that ensures security and operational stability through continuous, intelligent monitoring. Thanks to state-of-the-art log and analysis methods, we detect potential risks at an early stage and can take proactive measures to ensure the availability and security of your systems.



4.3.1 Log aggregation and analysis

Effective log management is the key to being able to track and analyze security and operational events in real time. Our central log management system collects and consolidates data from various sources to enable a well-founded and holistic analysis. We rely on automated processes that also cover long-term requirements such as forensics and compliance. Our central log management system offers:

- **Real-time recording and aggregation of all system logs**
- **Correlation of different log sources for holistic analysis**
- **Long-term archiving for forensics and compliance**
- **Intelligent filter mechanisms to reduce false positives**
- **Ensuring the integrity and confidentiality of log data by using established tools.** We rely on proven logging and monitoring tools such as Prometheus and Grafana for metrics and OpenSearch Dashboards for log aggregation and analysis. This enables scalable and powerful processing of large volumes of data.

4.3.2 Metrics and Alerting

With our integrated metrics and alarm system, we ensure that critical events are detected and addressed immediately. Precise monitoring of relevant parameters and automatic notification of anomalies enable us to guarantee continuous operational reliability and minimize disruptions.

- **Monitoring of critical system parameters**
- **Real-time-based alerting when limit values are exceeded**
- **Multi-level escalation paths for different event types**
- **Automatic notification of the responsible support team**
- **Trend analyses for early detection of potential problems**

This comprehensive monitoring infrastructure enables us to identify potential problems at an early stage and rectify them before they can affect your operations. In this way, we ensure that security standards, compliance requirements and operational stability are consistently maintained at all times.

4.4 Regular audits

The systematic review of all security-relevant aspects is a fundamental part of our security concept. With regular audits, we ensure that all systems are optimized and further developed in accordance with the highest safety standards. This approach not only gives us the opportunity to validate existing processes, but also to identify potential areas for improvement at an early stage.

4.4.1 Comprehensive safety checks

Our audits follow a clear and structured audit plan aimed at a holistic analysis of safety-critical issues. In this way, we ensure that all technical and organizational measures remain up to date. Our regular audits include:

- **Detailed review of all system configurations**
- **Audit of access rights and user accounts**
- **Evaluation of implemented security settings**
- **Validation of backup and recovery processes**
- **Assessment of the patch level of all systems**

4.4.2 Structured documentation

The results of each audit are recorded transparently and documented systematically. This not only ensures traceability, but also enables targeted follow-up of the identified measures and findings. All audit processes are recorded in our central documentation system:

- **Complete logging of all checks**
- **Comprehensible documentation of findings**
- **Tracking of improvement measures**

Through these regular and documented audits, we not only ensure the current security of our systems, but also create a solid basis for future security optimizations. At the same time, we always aim to continuously increase our security level and respond appropriately to new challenges.

4.5 User authentication

For all administrative access, M2MGate implements a multi-layered authentication system that combines maximum security with user-friendliness. By combining established security mechanisms with a focus on ease of use, we protect your systems from unauthorized access while promoting efficient workflows and reducing security risks in the long term.

4.5.1 Multi-Factor Authentication (MFA)

Multi-factor authentication is a central component of our security concept. It combines different security methods to reliably verify the identity of users. This ensures that unauthorized access is prevented even if access data is compromised. The mandatory MFA offers several levels of security:

- **Combination of knowledge (password) and possession (token/smartphone)**
- **Currently used as a second factor: Time-based One-Time Passwords (TOTP)**
- **Protection against compromised access data**
- **Prevention of unauthorized access even with known passwords**
- **Detailed logging of all authentication attempts**

4.5.2 Single Sign-On (SSO)

The integration of Single Sign-On (SSO) simplifies access to various systems considerably. A single authentication process is all that is needed to enable access to all relevant applications. At the same time, the protection of your data is guaranteed at all times by central security mechanisms. The integration of SSO optimizes access:

- **One-time, secure authentication for all systems**
- **Reduction of password fatigue**
- **Central administration of access rights**
- **Automatic blocking when employees leave**
- **Simplified access management**

This combination of MFA and SSO ensures that administrative access is optimally protected, while at the same time enabling efficient work.

4.6 Data integrity and backups

The protection and availability of your data is a top priority at M2MGate. Our comprehensive backup and recovery strategy ensures the integrity and rapid recoverability of all business-critical data. We use both automated processes and project-specific adjustments to secure your data reliably and for the long term - regardless of any challenges that may arise.

4.6.1 Robust backup strategies

To effectively prevent data loss, we rely on an automated and multi-layered backup system. Through regular backups, comprehensive integrity checks and clear recovery mechanisms, we ensure the continuous availability and protection of your data. Our automated backup system offers:

- **Regular, automated backups of all relevant data**
- **Multi-layered backup architecture (daily incremental backups and weekly full backups)**
- **Continuous integrity checks**
- **Automatic verification of backup completeness**

4.6.2 Project-specific adaptations

Our backup and recovery strategy is flexibly designed to implement individual customer requirements without compromise. We ensure that the backup processes are aligned with the specific business requirements and technologies of our partners.

- **Individual backup frequencies according to business requirements**
- **Customizable retention periods**
- **Flexible recovery options**
- **Scalable storage capacities**
- **Tailor-made service level agreements**

This multi-layered protection of your data ensures that your business operations can continue with minimal disruption, even in exceptional situations.

5 SAFETY CHECK AND CONTINUOUS IMPROVEMENT

The security architecture of M2MGate is based on the principle of continuous review and adaptation. As security is a dynamic field that requires constant vigilance, we use systematic checks, effective incident management and continuous improvement to ensure that M2MGate is always prepared for the latest threats and meets high security standards.

5.1 Systematic safety checks

5.1.1 Security as an integral part of system development

The security of our platform is embedded in the development process right from the start. Security aspects are already taken into account and systematically implemented during the planning and design phase. By consistently integrating security-relevant measures in all phases of software development, we ensure that our information systems are robust and resistant to threats from the ground up. This preventive approach creates a sustainable security architecture that goes far beyond selective checks. Among other things, the following measures are implemented:

Automated security scans: Regularly perform automated vulnerability scans for early detection of potential security vulnerabilities in code.

Internal code reviews: Review of source code within development according to the dual control principle, with a focus on security-critical components.

Infrastructure audits: Review of underlying infrastructure components for security updates, configuration errors and best practice compliance.

Architecture reviews: Review of the system architecture for security vulnerabilities and implementation of current security standards. By integrating these security checks into our development cycle, we ensure that security is not added as an afterthought, but is considered from the outset.

5.1.2 External security validation on customer request

As an additional quality assurance measure, we support the performance of external penetration tests and code audits by independent security experts at the customer's request. These objective third-party audits provide valuable insights and confirm the effectiveness of our security measures.

The external audits requested by customers in the past have repeatedly confirmed the robustness of our security architecture. These independent validations are particularly valuable as they look at the platform from the perspective of potential attackers, providing insights that internal testing may not reveal. The external audits typically include:

- **Penetration tests:** Simulation of real attacks on the M2MGate platform to identify and evaluate potential vulnerabilities.
- **Code audits:** Review of source code for security vulnerabilities, adherence to best practices and compliance requirements.
- **Detailed reporting:** Documentation of the audit results with specific recommendations for optimization.
- **Validation of remediation:** After implementing improvement measures, a follow-up audit is carried out if required.

Especially for customers with regulatory requirements, these external checks offer additional security and often fulfill compliance requirements for the use of IoT platforms in safety-critical areas.

5.2 Incident management: fast and effective response

Despite preventative measures, it is essential to be prepared for potential security incidents. Our incident management process ensures a structured and effective response to protect system integrity.

5.2.1 Post-mortem analysis

The systematic evaluation of security incidents and test results is a central component of our continuous improvement process. Through post-mortem analysis, we gain valuable insights that help to strengthen our security architecture.

After every significant security incident or major security audit, we carry out a comprehensive analysis that goes beyond immediate problem solving. This structured process allows us to learn from experience and implement systemic improvements:

- **Root cause analysis:** We not only identify the immediate triggers of an incident, but also investigate the underlying systemic factors that may have contributed to it.
- **Process analysis:** The effectiveness of our response is critically examined in order to identify optimization potential in our security processes.
- **Development of measures:** Based on the findings, we develop specific improvement measures, which can include both technical and procedural aspects.
- **Knowledge transfer:** The results of the analysis are documented and shared with relevant teams in order to strengthen collective security awareness.
- **Integration:** Identified improvements are systematically integrated into existing processes and guidelines.

This reflective approach allows us to look beyond individual incidents and gain deeper insights into potential security risks. Post-mortem analysis closes the loop in our security management and ensures that every experience contributes to strengthening overall security. In practice, this process has repeatedly led to significant improvements in our security architecture.

5.3 Continuous improvement

The continuous improvement of our security measures is not an isolated process, but an integral part of our corporate culture. We view security as an evolutionary process that requires constant attention, adaptation and further development.

We counter the constantly changing threat landscape with a dynamic security concept that proactively responds to new challenges. Our experts continuously monitor current security trends and threats in order to be able to make adjustments at an early stage. These findings flow directly into our improvement cycle.

Based on the results of our internal and external security audits and the findings from incident management, we develop targeted optimizations in various areas:

- **Ongoing adaptation of our security standards:** We regularly adapt our security standards to new threats and best practices to ensure a contemporary security framework.
- **Improved preventive measures:** New findings lead to the implementation of additional security-barriers and the optimization of existing protective measures.
- **Optimized response processes:** Lessons learned from past incidents help us to continuously improve our response capabilities and shorten response times.
- **Enhanced monitoring strategies:** We continuously refine our monitoring mechanisms to detect suspicious activities even earlier.
- **Adapted training content:** Our team receives regular training on current security topics to promote security awareness at all levels.

These improvements are not integrated in isolation, but as part of a holistic approach that takes into account technical, organizational and human factors. Regularly reviewing the effectiveness of these measures creates a self-reinforcing cycle of continuous optimization.

This comprehensive approach to security testing and incident management enables us to respond proactively to new threats and continuously improve our security measures. The combination of internal processes and external validation ensures that M2MGate provides a robust and trustworthy platform for your IoT solutions - today and in the future.

INSIDE M2M
SMART MACHINES

INSIDE M2M GmbH
Phone: +49 (0) 5137-90 95 0-0
Mail: vertrieb@inside-m2m.de

inside-m2m.de

Garbsen
Berenbosteler Straße 76 B
30823 Garbsen

Bissendorf
Gewerbepark 9-11
49143 Bissendorf

Berlin
Marienburger Straße 1
10405 Berlin