METER

SKALA® CONTROL SECURITY, PRIVACY, AND ARCHITECTURE

Published: March 2020

METER CORPORATE COMMITMENT TO TRUST

The trust of METER customers is critical to us, and we are committed to achieving, and maintaining that trust. To that end METER considers it integral to provide a robust security and privacy program that carefully considers data protection matters, including protection of Customer Data.

SERVICES INCLUDED

This documentation describes the architecture of the security and privacy-related audits and the administrative, technical, and physical controls applicable to (1) SKALA Hardware (including NEXUSes and Hubs) and (2) SKALA Control (collectively, referred to for the purposes of this document only as "Covered Services").

ARCHITECTURE AND DATA SEGREGATION

The Covered Services operate in a multitenant architecture, which is designed to segregate and restrict customer data access based on business needs. The design of the system allows for an effective and logical data separation for different customers via customer-specific Site IDs and allows the use of customer and user-based, role-driven access privileges. Further additional data segregation is ensured by providing unique purpose-driven environments for different functions, such as testing, development, and production.

PROCESSING CONTROLS

SKALA has been implemented and designed to ensure that Customer Data is processed, only as instructed by the customer, throughout the entire chain of processing activities and any subprocessors. METER has entered into written agreements with our subprocessors and service providers that include privacy, data protection, and data security obligations aimed at providing a level of protection appropriate to the processing activities.

AUDITS

The covered services undergo security assessments by internal personnel and third-party security experts, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis.

SKALA uses infrastructure provided by Amazon Web Services, Inc. ("AWS") to host Customer Data submitted to SKALA. Information about the AWS security and privacy audits, and certifications, including ISO 27001 and SOC reports, is available at the AWS Compliance Website and the AWS Security Website.

METER also audits for compliance where appropriate. Please see the Certifications section below for more details.

CERTIFICATIONS

SKALA is an FDA 21 CFR Part 11 compliant system. METER is audited by an external third-party auditor for Part 11 compliance, and we have achieved a perfect score. A copy of our audit report is available upon request.

SECURITY CONTROLS

The Covered Services include configurable security controls that allow customers to tailor the security of the Covered Services for their own use. Please see additional information about these controls in the SKALA User Security Guide.

METER Group, Inc. USA
2365 NE Hopkins Court, Pullman, WA 99163
T +1.509.332.2756 **F** +1.509.332.5158
E info@metergroup.com **W** metergroup.com

SECURITY POLICIES AND PROCEDURES

The Covered Services are operated in accordance with the following policies and procedures to enhance security:

- Customer Passwords are stored using a one-way, salted hash.
- User Access Log Entries will be maintained, containing date, time, user ID, URL executed or entity ID operated on, operation performed (Create, Update, Delete), and source IP address. Note that source IP may not be available if the customer is using NAT or PAT.
- If there is suspicion of inappropriate access, METER can provide customers log entry records.
- Data Center Physical Access logs, System Infrastructure logs, and Application logs will be kept for a minimum of 90 days. Logs will be kept in a secure area to prevent tampering.
- Passwords are not logged.
- Administrative Changes to the Covered Services (such as password changes) are tracked in the event log and can be reviewed by the customer's administrative users.
- METER will not set a defined password for any users. Passwords are reset to a random value (which must be changed on first use) and delivered automatically via email to the requesting user.

SECURITY LOGS

All systems used in the provisioning of the Covered Services, including firewalls, routers, network switches, and operating systems, log information to their respective log facility or a centralized log server (hereto referred to as the SIEM) in order to enable security reviews and analysis.

INCIDENT MANAGEMENT

METER maintains security incident management policies and procedures. METER will notify any impacted customer without undue delay of any unauthorized disclosure of their respective Customer Data by METER or its agents of that METER becomes aware to the extent permitted by law.

METER typically notifies customers of significant incidents by email and, for incidents lasting more than four hours, may invite customers to join a conference call about the incident and METER's response.

USER AUTHENTICATION

Using the Covered Services requires authentication via one of the supported mechanisms described in the SKALA User Security Guide. All data access requires successful authentication. Following successful authentication, the system will assign a random session ID to the user's browser to preserve and track session state.

ACCESS CONTROLS

SKALA operates under a least-privilege access model. This model is extended to METER developers, IT, and support staff. In order to ensure that this model is applied appropriately and that the Customer Data is protected, METER has implemented a number of technical controls around access to the systems and Customer Data. These technical controls include tightly controlled IP whitelisting, Key-based SSH access, minimal port availability, and an auditable recorded remote access tool ensuring that all activities taken by METER staff are accountable, traceable, and appropriate.

PHYSICAL SECURITY

Production data is housed in a data center that utilizes access control systems to ensure only authorized personnel have access to secure areas. These facilities are designed to withstand adverse weather, provide redundant electrical and telecommunication systems, utilize environmental monitoring systems to monitor temperature, humidity, and other conditions, and contain strategically placed heat, smoke, and fire detection and suppression systems. Facilities are secured by around-the-clock guards, surveillance, and two-factor access screening and escort-controlled access. In the event of a power failure, uninterruptible power supply and continuous power-supply solutions are used to provide power while transferring systems to on-site backup generators.

RELIABILITY AND BACKUP

All networking components and servers are configured in a redundant configuration. All Customer Data submitted to the Covered Services are stored on a primary database server with multiple active clusters for higher availability. All Customer Data submitted to the Covered Services, up to and including the last committed transaction, are automatically replicated on a near real-time basis to the secondary site and

backed up to localized data stores. The foregoing replication and backups may not be available in the case that a "Right to be Forgotten" request is submitted or the account is canceled or otherwise terminated because either may delete Customer Data submitted to Covered Services without the possibility of recovery.

VIRUS

The Covered Services will not scan for potential viruses included in attachments or other Customer Data uploaded into the Covered Services by a customer. Uploaded attachments, however, are not executed in the Covered Services and, therefore, will present no risk to damage or compromise of the Covered Services by containing a virus.

DATA ENCRYPTION

The Covered Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Covered Services, including through Transport Layer Encryption (TLS) leveraged at a minimum of 2048-bit RSA certificates and 128-bit symmetric encryption keys. All data transferred between data centers utilizes AES-256 encryption.

RETURN OF CUSTOMER DATA

There is a 30-day grace period post contract termination where customers may request the return of their respective Customer Data submitted to the Covered Services (to the extent that such data has not been deleted by the Customer). SKALA shall provide such Customer Data via a downloadable file in comma-separated value (.csv) format and attachments in their native format.

DELETION OF CUSTOMER DATA

Day 0	Contract termination—data are available for return to the customer.
Day 31	Data are inactive and no longer available for the customer.
Day 121	Data are deleted or overwritten from production.
Day 365	Data are deleted or overwritten from backups.