

KDC Client

Automated Key Management for Secure GOOSE and Sampled Values

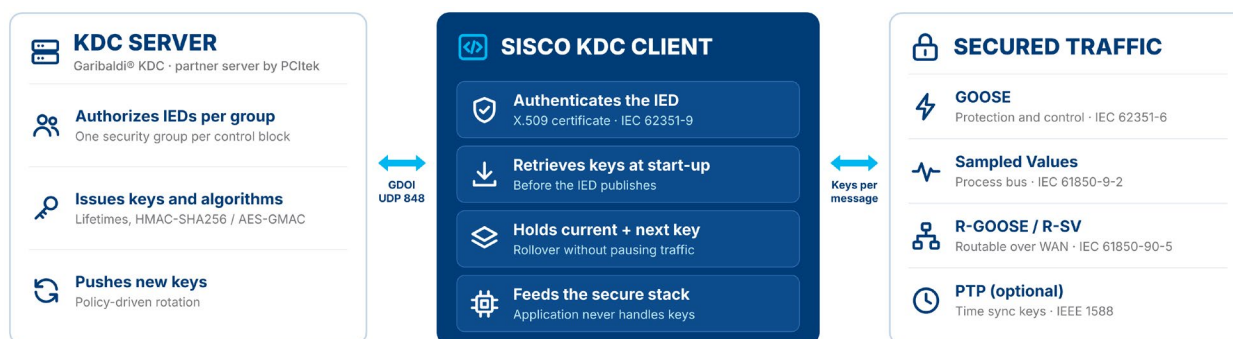
IEC 62351 protects GOOSE and Sampled Values with shared cryptographic keys, but every publisher and subscriber in a group must hold the same valid key at all times. SISCO KDC Client automates that job. Built to IEC 62351-9, it authenticates each IED to a Key Distribution Center (KDC), retrieves the keys for every secured control block, and renews them before they expire. Protection traffic stays signed and encrypted, and no engineer handles key material.

The Challenge: Multicast Security Does Not Scale by Hand

GOOSE and Sampled Values carry trip signals and process measurements that cannot wait. Because they are multicast, point-to-point security such as TLS does not apply: every device in a group must share one key. Managing those keys by hand across dozens of IEDs and substations leads to expired keys, missed rollovers, and incomplete audit evidence. IEC 62351-9 solves this with a central KDC and the GDOI protocol, but each IED needs a client that speaks it.

Why It Matters

- **IED and gateway manufacturers:** Add IEC 62351-9 key management to your products through a C API instead of building GDOI from scratch. KDC Client is integrated with SISCO 61850 PLUS, or operates stand-alone for other applications.
- **Protection and substation automation engineers:** Secure GOOSE and Sampled Values from the SCD file you already maintain. Keys roll over without interrupting traffic.
- **OT security architects:** Enforce group-level authorization from central KDC server. Each IED must authenticate with an X.509 certificate before it receives a key.



Key Capabilities

- **Keys ready before first publish.** Obtains keys for every secured control block at start-up, then keeps them current through KDC push or a fresh pull before expiry.
- **Hitless key rollover.** Keys arrive as current and next pairs. Publishers switch at the next key's activation time, so rollover needs no pause in traffic.

- **SCL-driven configuration.** Reads the SCD and secures each GSEControl and SampledValueControl block per its securityEnable setting (Signature or SignatureAndEncryption), so security lives in the same engineering file as the substation.
- **Per-group isolation.** Each control block forms its own security group with its own keys. A 32-bit key ID in every message tells subscribers which key to apply.
- **No key handling in application code.** Keys pass directly to SISCO's secure GOOSE/SV stack.
- **Layer 2, routable, and time sync.** Secures Ethernet GOOSE and SV (IEC 62351-6), routable R-GOOSE and R-SV (IEC 61850-90-5), and optionally PTP (IEEE 1588).
- **Fail-closed option.** Hold transmission and drop unsigned messages until valid keys arrive.

Security

- **Device authentication:** Each IED authenticates with an X.509 certificate before receiving keys.
- **GOOSE and SV protection:** HMAC-SHA256 or AES-GMAC signatures, with optional AES-CBC or AES-GCM encryption. The KDC assigns the algorithm with each key.
- **KDC exchange:** AES-CBC, SHA2-256, and RSA signatures; Diffie-Hellman groups MODP_1024 to MODP_8192 (MODP_2048 or higher recommended).

Standards and Specifications

- **Key management:** IEC 62351-9 (GDOI PULL and PUSH)
- **Message security:** IEC 62351-6; IEC 61850-90-5 (R-GOOSE, R-SV)
- **Traffic secured:** GOOSE (IEC 61850-8-1), SV (IEC 61850-9-2), PTP (IEEE 1588, optional)
- **Configuration and network:** IEC 61850 SCL (SCD) plus one startup file
- **Integration:** C API; integrates with SISCO 61850 PLUS – or standalone for other applications

Ecosystem Partner: Garibaldi® KDC by PCitek

KDC Client is the device side of IEC 62351-9 key management; Garibaldi® KDC is the server side. Garibaldi adds central policy, RADIUS-based access control, failover, and audit logging.

Why SISCO

SISCO engineers participate in the IEC TC57 working groups that define IEC 61850 and IEC 62351 security. Since 1983, SISCO has delivered standards-based integration for IEC 61850, IEC 62351, IEC 61850-90-5, IEC 61850-9-2, and CIM, with global support behind every license.

KDC Client comes from the team behind 61850 PLUS.

Get Started

Ready to secure GOOSE and Sampled Values? Contact SISCO to request a demo, discuss integration, or talk with the engineers who built KDC Client.

Email: sales@sisconet.com | **Web:** sisconet.com | **Phone:** +1 (586) 254-0020