Jornadas Técnicas

Industrial Track 4.0

2024

ILOQ TECNOLOGIA DE CONTROL DE ACCESOS SIN BATERIAS CUMPLIENDO NIS2

BURGOS, 24-25 DE SEPTIEMBRE 2024

AGUSTIN HIGUERA – NORTH SPAIN AND PORTUGAL SALES MANAGER

iLOQ

iLOQ en breve

SOBRE 320
EMPLEADOS

141,3 MILLONES
FACTURACIÓN 2023

SOBRE **3 MILLONES** CILINDROS
5 MILLONES LLAVES ENTREGADAS

SIN BATERÍAS NI CABLES
SOLUCIONES DE CONTROL DE ACCESO DIGITAL Y MÓVIL

100 000 KG
DE BATERÍAS AHORRADAS
CADA AÑO

OFFICINA CENTRAL
OULU, FINLAND

FUNDADA EN
2003

OPERANDO EN
55 PAÍSES

CERTIFICADOS

ISO 9001:2015	Certificado Calidad
ISO 14001:2015	Certificado Ambiental
ISO/IEC 27001:2013	Gestión Segura de los Sistemas de Información

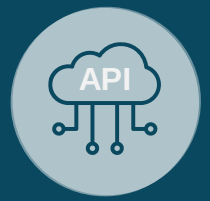
iLOQ 5 Series

Aplicaciones de programación

Software
iLOQ Manager

Aplicaciones iLOQ
para teléfono

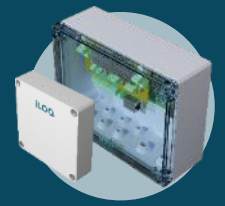
Equipo de programación
iLOQ



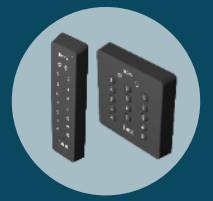
Interfaz
de programación
de aplicaciones
iLOQ

Productos Online

Módulo de puerta
iLOQ con
conectividad 4G



Puente de red y
módulo de puerta
iLOQ
para la conectividad
con cable

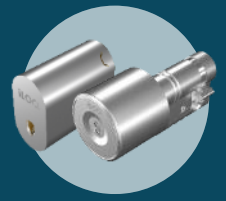


Lectores
iLOQ Online

iLOQ S5

Catálogo de productos

Llave iLOQ S5



Cilindros iLOQ

Cilindros de tubo
de llave iLOQ

Candados iLOQ

Cilindros de leva iLOQ

iLOQ S50

Catálogo de productos

Llaves iLOQ S50

Cilindros iLOQ

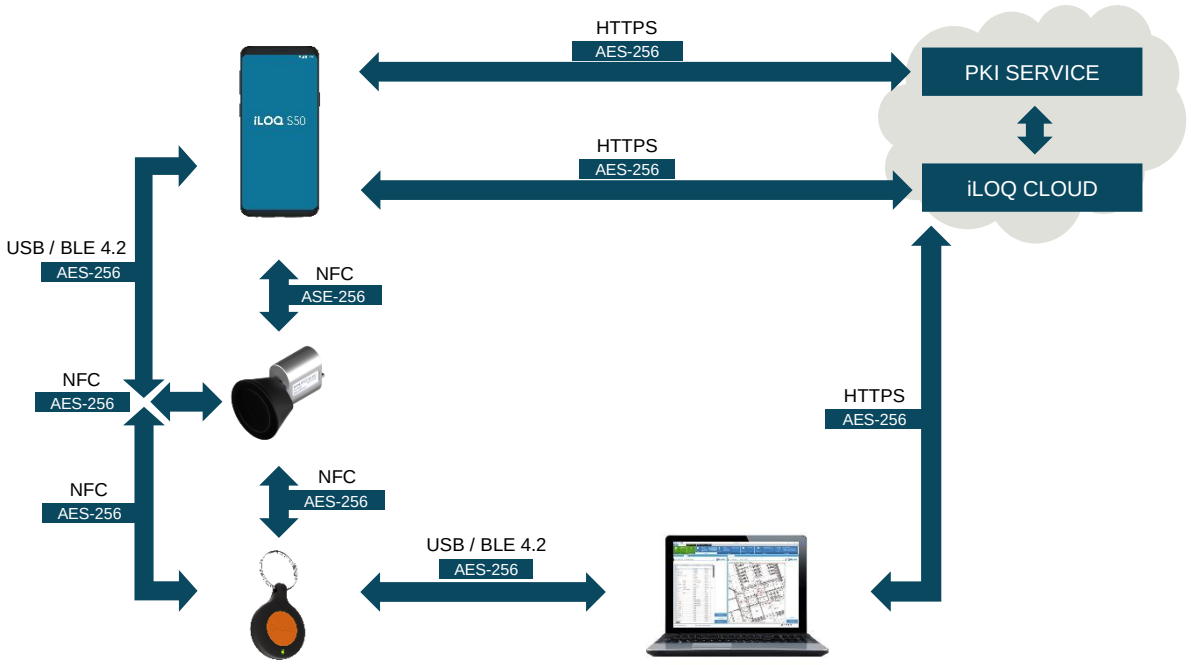
Cilindros de tubo
de llave iLOQ

Candados iLOQ

Cilindros de leva iLOQ

Seguridad de última generación

- PKI (Public key infrastructure)
- Autenticación mutua entre la llave y la cerradura mediante encriptación AES-256
- Protección de la App frente a malware y uso indebido
- Cumple los requisitos de la norma europea EN15684 para resistencia al ataque, corrosión y durabilidad.
- ISO27001:2015 certificación del cloud server
- La nube solo almacena datos administrativos con opción de uso de datos no criticos
- Token de programación requerido para cerraduras de seguridad críticas
- Doble sistema de identificación con autenticación continua.
- Huella de tiempo y trazabilidad de todas las operativas incluso en caso de corte eléctrico o de comunicaciones.
- Compatible con normativa DARA y CER (Directiva europea de resilencia de entidades críticas).



iLOQ ha desarrollado una tecnología que resuelve estas problemáticas

Otros

- ✗ Necesitan mantenimiento
- ✗ Muchas llaves / Dos sistemas: Mecánico y digital
- ✗ Imposibilidad de controlar las copias
- ✗ Requiere custodia de llaves
- ✗ Llaves diferentes para zonas diferentes
- ✗ Sistemas muy caros de implementar
- ✗ Limitación de combinaciones
- ✗ Rigidez a la hora de realizar cambios
- ✗ Requieren fuentes de energía externas
- ✗ Generación de residuos nocivos para el medio ambiente

iLOQ

- ✓ No necesita de ningún mantenimiento (garantizado)
- ✓ Un único sistema de control de acceso.
- ✓ Imposible de copiar sin autorización
- ✓ No es necesaria la custodia de copias de llaves
- ✓ Una sola llave para acceder a todas las zonas
- ✓ Implementación amortizable a lo largo del ciclo de vida
- ✓ Prácticamente infinitas combinaciones
- ✓ Sistema completamente rediseñable
- ✓ No requiere cableados ni baterías para funcionar
- ✓ La perdida de una llave no afecta los cilindros ni a otros usuarios
- ✓ Completamente respetuoso con el medio ambiente

NIS2

https://nis2directive.eu/

Expanded scope NIS 2 Directive

NIS 1 and NIS 2

- ENERGY
- HEALTH
- TRANSPORT
- DRINKING WATER
- BANKING
- DIGITAL INFRASTRUCTURE
- FINANCIAL MARKET INFRASTRUCTURE
- DIGITAL SERVICE PROVIDERS

NIS 2 additional sectors

- FOOD
- MANUFACTURING
- POSTAL & COURIER
- PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR SERVICES
- ICT SERVICE MANAGEMENT
- WASTE WATER
- WASTE MANAGEMENT
- PUBLIC ADMINISTRATION
- SPACE
- RESEARCH
- CHEMICALS

4

Incident Notification

NIS2 imposes notification obligations in phases, for incidents which have a 'significant impact' on the provision of their services. These notifications must be made to the relevant competent authority or CSIRT (Computer Security Incident Response Team).

24h — EARLY WARNING
Is it a suspected malicious act with potential cross-border impacts?

↓

72h — OFFICIAL INCIDENT NOTIFICATION
Assessment of the incident, severity and impact, plus indicators of compromise.

↓

as requested — INTERMEDIATE STATUS REPORT
At the request of CSIRT or relevant competent authority.

↓

1 month — FINAL REPORT
Or if incident ongoing at time of final report a progress report and final report 1 month after end

Where appropriate, entities shall notify the recipients of their services of significant incidents.

When in the public interest, the CSIRT or relevant competent authority may inform the public about the significant incident or may require the entity to do so.

5

Cyber Security Risk Management Measures

Essential and Important entities must take appropriate and proportional technical, operational and organisational measures to manage the risks posed to the systems which underpin their services, and prevent or minimise the impact of incidents on their and other services.

Such measures shall be based on an all-hazards approach that aims to protect the network and information systems and the physical environment of those systems from incidents, and must include at least the following:

1. Risk analysis & information system security
2. Incident handling
3. Business continuity measures (back-ups, disaster recovery, crisis management)
4. Supply Chain Security
5. Security in system acquisition, development and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk management measures
7. Basic computer hygiene and trainings
8. Policies on appropriate use of cryptography and encryption
9. Human resources security, access control policies and asset management
10. Use of multi-factor, secured voice/video/text comm & secured emergency communication

All measures must be:

- Proportionate to risk, size, cost, and impact & severity of incidents
- Take into account the state-of-the-art, and where applicable relevant European and international standards

EU can:

- Carry out risk assessments of critical ICT services, systems or supply chains
- Impose certification obligations (delegated acts)
- Adopt implementing acts laying down technical requirements

iLOQ Life made limitless.

Agustin Higuera
agustin.higuera@iLOQ.com
+34 699 27 14 14