Iskratel Intelligent Applications Platform for Energy (IAPE)

Cybersecurity for energy data intelligence platform

Key features

- **Secure development**
- **Strong authentication**
- **Role-based access control**
- **Software-defined perimeter**

Why Iskratel?

- **Own R&D** and EU-based **manufacturing**
- **First** integration **pilot** on a national level in EU
- **70 years** of Iskratel experience

Iskratel IAPE simplifies and optimizes IT and OT integration and convergence in a standard manner and as such is one of the core energy utility systems. Number of cyber-attacks is rising, so this is a very crucial segment which is excellently covered within the solution.

SECURE DEVELOPMENT

Cybersecurity is an integral part of the IAPE. It is not treated as an additional feature added on top of the solution at the end, but it is incorporated into systems development life cycle which makes the whole solution secure at all levels.

STRONG AUTHENTICATION

In order to access different features of IAPE you need to go through strong authentication. This is required for users who use Web Apps via using APIs, as well as for machines and edge devices connecting to the platform through Web Services or message brokers.

IAPE supports common authentication types and also combination of them, which forms multi-factor authentication:

- Username/password
- X.509 client certificate
- One-time password

IAPE can be integrated with existing client's authentication solutions such as Kerberos and LDAP, often found in Windows domain environments and others, therefore providing user federation and optionally single sign-on.

Existing client's identity provider (IdP) solutions can also be leveraged for authentication and authorization as well, thus acting as an identity broker. Supported and often used enterprise IdPs include:

- SAML v2.0
- OIDC v1.0

STRICT AUTHORIZATION

Each feature has controlled access implemented through role-based access control, which is IAPE's primary authorization mechanism. Roles and privileges can be mapped to groups and synced from client's directory services like Microsoft AD or other LDAP services. Roles-mapping with directory services groups can leverage existing groups; therefore no changes are required at customer's directory services configuration.

SERVICE PROTECTION

Publicly or widely accessible services are additionally protected using Software Defined Perimeter (SDP), which effectively mitigates network attacks, most notably DoS and DDoS attacks.

Benefits

- **Full stack security** Incorporated into every single stage
- All communications are **encrypted**
- **Secure integration** into customers environment
- Compliant with **industry standards**

DATA ENCRYPTION/PROTECTION

All communications between IAPE and external systems and clients are encrypted using transport layer security (TLS) to prevent man-in-the-middle attacks. TLS is supported with a standalone public key infrastructure (PKI), or existing client's PKI can also be used. Together with the high-availability setup of critical components the solutions fulfills fundamental security aspects:

- Confidentiality
- Integrity
- Availability

THREAT MODEL

Through threat modelling and threat assessments, we identified critical threats to IAPE. In order to mitigate or lower the risk of successful data breach, the most important being were taken into consideration:

- Hardening of hardware, cloud platform, operating systems, application servers, platforms and frameworks
- Secure coding
- Security verification

CYBERSECURITY VERIFICATION

Security verification is being performed with regular:

- Security design reviews
- Code reviews
- Vulnerability assessments
- Penetration tests (pentests)

DEFENCE IN DEPTH

Security is built into many logical layers of the solution. Each layer provides an obstacle for potential attackers to hack into the platform. The key layers are:

- Network / communication security
- Host / system security
- Application security
- Data security

MANAGEMENT & COMPLIANCE

System and software security is managed and monitored through Software Assurance Maturity Model framework, which defines twelve security practices for core business functions of software development. All taken security measures make IAPE compliant with approved industry cybersecurity standards.

SECURE INTEGRATION

Cybersecurity of the final IAPE deployment depends on the level of integration into the existing client's environment, as well as the security of the platform itself. Our certified experts provide consultancy and integration services that assure proper and secure integration into customer's environment.

Iskratel, d.o.o., Kranj

Ljubljanska cesta 24a
SI 4000 Kranj, Slovenia
Phone: +386 4 207 20 20
Fax: +386 4 207 26 06

info@iskratel.si
www.iskratel.com