



Solution Architect with cybersecurity/cryptography experience | Contract

HITCONTRACT

www.hitcontract.lt

Lietuva

Apie poziciją:

Vietovė

Vilnius, Lietuva

Atlyginimas (Įrankas)

€6700 - 8700/Mėn.

Trukmė

Igalaikis projektas (>12 mėn.)

Extension (project)

Taip

Remotely (optionally)

Taip

Galioja iki

2026-08-31 (Už 4 savaites)

Aprašymas

We are part of an organisation which delivers world-class digital financial solutions to customers. We understand that change is Technology-driven and that IT is a key component for success in our journey to drive digital disruption in the bank. Our teams work with complex tech challenges and develop Danske Bank's global competitive edge on innovative digital solutions.

Responsibilities:

- Work with internal stakeholders and define the end-to-end solution architecture for the cryptographic inventory, including discovery, ingestion, normalisation, enrichment, validation, reporting and lifecycle management of cryptographic assets.
- Security architecture and design: Design the target data model covering certificates, keys, algorithms, protocols, cipher suites, key stores, trust stores, HSMs, KMS services, secrets platforms, ownership, criticality, expiry, compliance status and exceptions.
- Define and validate integrations with key source systems such as CMDB, application portfolios, PKI, certificate lifecycle tools, HSMs, cloud KMS, secrets managers, CI/CD pipelines, vulnerability

tools, GRC and SIEM platforms.

- Stakeholder collaboration: Work with a variety of stakeholders including third parties, product vendors, leadership, peers in the security organisation and across the Danske Bank group and establish ownership and governance models for cryptographic assets, communicate complex security topics in a clear, business relevant way.
- Define security controls for the inventory platform, including access management, privileged access, segregation of duties, audit logging, encryption, monitoring and secure administration.
- Regulatory and compliance alignment: Work with security requirements and support compliance to ensure the solution contribute to internal and external compliance and regulatory requirements.
- Support security engineering teams by reviewing designs, advising on configuration, validating integrations, supporting testing and ensuring the solution is ready for production.
- Continuous improvement: Facilitate architecture assurance, risk assessments and threat modelling to ensure the solution meets security, audit, operational resilience, data protection and third-party risk requirements.

Requirements:

- Solid working understanding of cryptography, including encryption, signing, hashing, certificates, PKI, key lifecycle management, HSMs, KMS platforms, cipher suites and cryptographic protocols.
- Broad hands-on knowledge of application, infrastructure, cloud, hybrid environment and network security, including secure design principles and common control requirements.
- Experience working with stakeholders across the organisation in designing secure integrations using APIs, connectors, or event-driven patterns across enterprise platforms.
- Desirable certifications include CISSP, CCSP, CISM, SABSA, TOGAF, ISO 27001 Lead Implementer or Lead Auditor.
- Advanced diplomatic and communication skills in English.

Senior-level, +5 years or more of solution architecture experience in large, complex organisations, preferably

designing enterprise asset, configuration, or inventory platforms.

We Offer:

- An inspiring environment in a large IT organization.
- Work in an international team, which concentrates on innovative business-facing solutions.
- An extensive training program to ensure that your skills are maintained and updated on an ongoing basis.

Preferred start date: ASAP, 12-month assignment with the possibility to extend.

On-Site in the Lithuania area (3-5 days On-Site, Vilnius, Lithuania).



Required Skills

REALIZACIJA

Solution Architecture 5-6 metai