CARSTEN SCHWANT

IAM & PKI SECURITY ARCHITECT

ABOUT ME

+49 151 506 252 73

carsten.schwant@bxc-consulting.com

https://www.bxc-consulting.com

Wagnerweg 1
85399 Hallbergmoos

With more than 15 years of experience in different Dax30 enterprises, Carsten worked in multiple disciplines of Cyber Security in particular in the areas of Identity and Access Management and PKI. He took over different types of roles among others: security engineering, project leadership, strategy and governance roles.

As Cyber Security specialist for IAM and PKI, Carsten consult and support international enterprises to find the most appropriate solutions for their cyber security challenges in IT and OT environments.

PROFESIONAL EXPERIENCE

LANGUAGE

German	Native
Englisch	Fluent

SOFT SKILLS

Project experience

5 years 10 years 15 years

Project leadership

5 years 10 years 15 years

International project

5 years 10 years 15 years

Collaboration skills

People management

Communication skills

Intercultural skills

Sep 2020 – Today
BxC Consulting
Founder

Since the founding of BxC Consulting, Carsten has been consulting companies based on the analysis of their requirements and developing solutions for secure IT and (I)IoT architectures. In parallel, he also took an active role in the strategic development of BxC Consulting.

Project experiences

International consumer goods producer
IAM & PKI Architect
Responsibilities: Implementing Factory CAs for the production of connected home appliances based on Nexus Smart ID product suite in customer's factory production lines. Defining the processes and their documentation of PKI administrative tasks to securely manage the different involved service components. Designing interoperational processes between PKI service components and customer's product development and supply chain.

International chemical industry company
IAM & PKI Architect
Responsibilities: Designing (I)IoT use cases for automated certificate lifecycle management connected factories and performing PoCs for selected ones. Establishing a high-level design for the IAM integration connected factories and make use of existing IAM capabilities in IT to ensure OT data authenticity, integrity and confidentiality.

Oct 2019 – Aug 2020
Carsten Schwant Consulting
Freelancer

Consulting international companies on IT and (I)IoT architectures in access management and PKI for secure device authentication and communication in heterogeneous environments.

Project experiences

International consumer goods producer
IAM & PKI Architect
Responsibilities: Designing and implementing an IoT PKI for connected home appliances based on Nexus Smart ID product suite including the creation of a high-level design and support during the phases of RfP and solution selection, technical implementation and documentation of the design. Extensive testing of PKI operational processes and cross-functional testing of the business use cases to ensure functional and security targets.

PROFESSIONAL EXPERIENCE

IAM SOLUTIONS

- Forgerock AM
- Forgerock OpenIG
- Sailpoint IIQ
- CyberArk
- Azure Identity

PKI / KEY MGMT.

- Microsoft PKI
- Entrust PKI
- Nexus PKI
- Venafi TrustAuthority
- Thales / Gemalto HSM
- Kryptus Knet HSM

PROGRAMMING / SCRIPTING

- Java
- Bash / Shell
- NodeJS
- Python

OFFICE TOOLS

- MS Word
- MS Excel
- MS PowerPoint
- MS Visio
- MS Projects

Carsten Schwant Consulting *(continued)*
Freelancer

Project experiences

International chemical industry company
IAM & PKI Architect
Responsibilities: Re-designing the existing enterprise-wide PKI and generation of future use cases for digitalization and (I)IoT. Generating of the solution design for an RFP of the future PKI solution and service and support as architect during the RFP. Defining the detail design for the implementation and integration of the new PKI service and performing PoCs to proof the design with selected solutions.

International automotive company
PKI Architect
Responsibilities: Designing and implementing an AD CS issuing CA for devices in a client's enterprise-wide storage/backup redesign project including the creation of a functional design and technical concept for the implementation of automatic lifecycle processes. Generating governance documents, such as CP (Certificate Policy) and CPS (Certificate Practice Statement) as well as implementing the issuing CA (Certificate Authority) and rollout of desired credentials to target service areas.

Sep 2018 – Sep 2019
Deloitte GmbH Wirtschaftsprüfungsgesellschaft
Senior Manager Cyber Risk

As a Senior Manager, Carsten was responsible to build IAM and PKI use cases for the Internet of Things and for enterprise business environments. Furthermore, he was successfully delivering several projects in international companies.

Project experiences

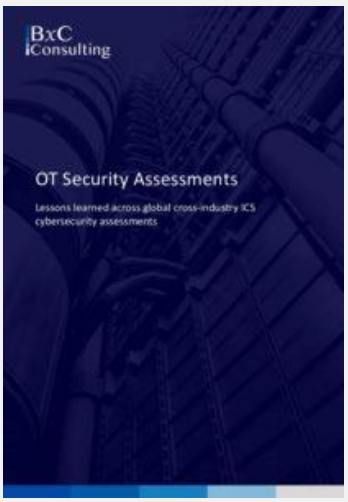
International insurance company
Project Manager
Responsibilities: Analyzing regulatory and Internal Control System requirements to establish an IAM and PAM practice. Designing the project roadmap and budget plan for the planned implementation and defining KPIs to measure the effectiveness of all established controls.

International industrial company
Project Manager and IAM / PKI SME
Responsibilities: Executing a Cyber Security assessment including gap analysis and remediation measures based on Deloitte methodology. Supporting the client to identify action plans and prepare an implementation roadmap to close identified gaps.

International processing industry company
IAM Architect
Responsibilities: Developing an IAM @ IoT Security Guideline for IAM related to IoT components in chemical production processes. Identifying areas of activities to initialize PoCs and lighthouse projects to justify the approach and prepare global reach.

International consulting company
IAM Architect
Responsibilities: Establishing a concept to design IAM services and an architecture for connected factories. Defining business use cases and implementing PoCs to test the use cases with available IAM solutions in enterprises. Developing of potential reference architectures for evaluation in international enterprises with the aim to converge IT and OT.

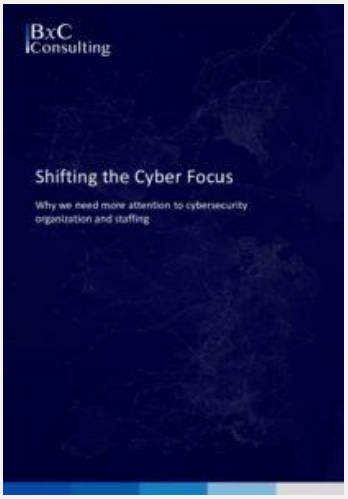
Selected Point of Views



OT Security Assessments

How do we navigate cybersecurity assessments in diverse and heterogeneous manufacturing environments?

Download



Shifting the Cyber Focus

Why are security departments failing to provide effective, sustainable and cost-effective protection for IT environments and production facilities??

Download

Aug 2016– Jun 2018
Deutsche Börse AG
Head of Identity and Access Management

Carsten lead the Identity and Access Management practice at Deutsche Börse Group and implemented various security controls to comply with regulatory requirements and improve the security posture of the group.

Responsibilities

Head of Identity and Access Management: Leading an international team of process and technology experts, as well as leading the IAM program organization. Acting as interface to business and C-level functions to include business demands into the IAM strategy and program, as well as providing reporting of internal and external compliance and threat environment status.

Identity and Access Governance: Defining end-to-end processes for secure and reliable identity and access information throughout the entire group. Implementing Sailpoint IIQ as IAG solution and connecting authoritative sources as well as target systems. Establishing effective provisioning and reconciliation processes and connectors to monitor the environment frequently and automatically. Designing and implementing a multi-layer business role concept to reflect business access control demand and ensure user friendly request and review processes.

Privilege Access Management: Evaluating existing operational processes and identifying risks for the business lines of the group. Defining a prioritized approach to decouple administrative work from business processes and establishing a security architecture for it. Implementing the Cyberark suite to ensure secure credential management of privileged user accounts and establish session monitoring for privileged user sessions. Integrating monitoring into the enterprise-wide SOC to foster rapid alerting for suspicious activities.

Access Management: Implementing an enterprise-wide access management solution based on the Forgerock product suite for modern and risk-based authentication of business users and software components via APIs. Succeeding legacy authentication solutions by providing user friendly and mobile authentication use cases for business users. Developing dedicated connectors for legacy applications, which did at that time not yet support modern authentication and authorization protocols.

Data Loss Prevention: Implementing controls to classify unstructured business data and process the classification during storage and sharing activities of business users in different file storage and collaboration environments. Establishing the Forcepoint service to enforce data loss control over data leaving the group's IT systems.

Oct 2012– Jul 2016
BASF Business Services (BASF Group)
Senior Security Architect (IAM & PKI)

As part of the Security Strategy and Architecture team of BASF Group, Carsten was responsible for governance work and lead as Lead Architect and Project Lead various projects of a global cyber security transformation program.

Responsibilities

Privilege Access Management: Evaluating the existing operational processes outlined the need for a holistic re-design of processes, dealing with privileged access to technical components and business applications of the BASF Group. Defining effective security measures, aligning with affected subsidiaries and operational functions and performing PoCs with potential solutions lead to the project scope to establish a Privilege Access Management solution. The implementation followed a risk-based approach to reduce the threat exposure significantly. The target was to secure privileged user accounts, their credentials and their correct use according to the internal and external regulations and operational processes.

Oct 2012– Jul 2016
BASF Business Services (BASF Group) ***(continued)***

Responsibilities

Access Management: Implementing an identity provider to enable the use of modern authentication and authorization protocols for the secure use of cloud-based services for business users and applications. Migrating existing applications and defining a new access management architecture to protect business applications from exposure to unnecessary networks.

Information Rights Management: Evaluating the demand and categories to classify business information and its protection effectively. Enforcing the protection by introducing an Information Rights Management solution, which classified unstructured and structured data. Adjusting business processes sharing information with internal and external communication partners ensured a higher protection against intended and unintended exfiltration of information to unauthorized parties.

Third Party Identity Management: Harmonizing the identity management processes of major sites. Defining joint registration, identity and company validation processes and implementing them in a globally available identity management solution. Developing an onboarding process supported further sites and business lines to leverage the system and streamlined global processes.

Modern Authentication: Optimizing the Multi-Factor Authentication environment and adding mobile-enabled and out-of-band authentication methods to support risk-based and user-friendly step-up authentication use cases for internal employees and external contractors.

May 2007– Sep 2012
BASF Business Services (BASF Group)
Security Solution Architect (IAM & PKI)

The role of Carsten included the technical lead of implementation projects for security solutions and their release into production. During their operational lifecycle, he was responsible for their secure and reliable operation and continuous improvement.

Responsibilities

Public Key Infrastructure: Re-designing the existing enterprise-wide PKI and integrating new requirements into certificate and service design. Technical implementation and the group-wide rollout of digital certificates to business users and devices. Turning the new service into operation and establishing service monitoring measures to ensure secure and reliable operation of key and certificate lifecycle processes.

Multi-Factor Authentication: Defining processes to securely authenticate business users for remote access and critical business applications. Technically integrating the MFA solution into business applications and setup the support for secure management of authentication tokens.

Smartcard: Assessing protection targets with secure key container solutions for business users. Evaluating different smartcard form factors and chips and implementing an enterprise-wide smartcard in combination with the company badge, already used for physical access and time tracking. Global rollout achieved strengthened credential management and improved the security posture by using strong authentication in many business applications, secure email and integrity protection of business information by enabling document signing use cases.

Munich, 01.11.2020

Carsten Schwant
BxC Consulting Founder