

Public Key Infrastructure [PKI] Service Offerings

• Planning and Implementation of Public Key Infrastructures

Design of scalable, multi-tier **hierarchies of certification authorities**, respective publication points, revocation services and interfaces with directory services. Integration of **Hardware Security Modules [HSMs]**. Establishing **cross-certification** with public CA vendors. Technical and organizational support with rollout of certificates to various clients and applications. Co-ordination with application owners, definition of **certificate lifecycle management processes**. Development and review of Certificate Practice Statements and Certificate Policies.

• PKI Workshops | PKI Consulting | PKI Client Support

Initial PKI workshop covering PKI and cryptography basics, hand-on implementation in Microsoft environments and heterogeneous environments. Interface technical/legal issues. **Examples:** Authentication of users and computers via 802.1x, smart card logon, file encryption, e-mail signature and encryption, signing of code and documents, authentication and encryption in VPN and IPsec. **Evaluation and selection of PKI enabled applications** and vendors. Analysis of existing applications and certificates.

• X.509-Troubleshooting and PKI Drill-Down

Problem analysis and fire-fighting in all issues related to X.509 certificates. **Review** | fixing of existing PKIs. **Train-the-experts workshops** and support for software vendors, security consultants and system integrators in the PKI area. Support with **application integration problems**, access to certificate and key stores, embedding specific certificate extensions and problems with **certificate path validation**. Evaluation of RFC compatibility. Co-ordination between vendors of PKI hardware and software in case of interface-related issues.

Engagements and Approach

Customers: Global corporations with more than 100.000 users and subsidiaries in more than 100 countries as well as local SMEs. More than 100 PKI consulting clients. PKI implementations done at about 50 clients.

Typical engagements: Bespoke PKI-related services. Work packages of 2-10 days.

Frequently encountered products and vendors: Microsoft and Verizon CAs, Verizon Omniroot root signing service. Windows clients. Smart cards/tokens: SafeNet, Siemens, Infineon. VPN concentrators, appliances, firewalls, MS IIS webserver.

Standards: X.509, SCEP, 802.1x, SMIME, LDAP, SSL, Kerberos

Methodology: Intensive know-how transfer in planning phase in order to make myself redundant, hands-on support in critical phases.

Vendor relations. Vendor-agnostic approach. Engagement as a subcontractor of vendors is an option if the product has already been selected. No solution sales, no deals based on commission, no IT staffing services providers.

Dipl.-Ing. Dr. Elke Stangl



Hands-on PKI experience since 2002. Self-employed since 2006. Senior Security Consultant at Microsoft Austria 2001-2005.

Experimental physicist with experience in: **R&D, IT management and IT consulting.**

Diverse **contacts to product vendors** and service providers in the PKI area – grown over many years.

Especially interested in **exotic PKI applications** and the convergence of IT infrastructure with building and logistics systems.