150 West Iowa Avenue
Suite 204
Sunnyvale CA 94086
(408) 331-2000
www.strongauth.com

Arshad Noor

StrongAuth, Inc., Sunnyvale, California

CHIEF TECHNOLOGY OFFICER, July 2001 to Present

Architected and built a **Public Key Infrastructure (PKI)** for the largest telecommunications company in the US, to secure 35,000+ Wi-Fi hot-spots across the country for strong-authentication. This PKI will issue one million digital certificates per year.

Architected, partially wrote and managed a team of developers to build and release **StrongKey CryptoEngine (www.cryptoengine.org)**, the industry's first free and open-source software (FOSS) to encrypt files of any size/type and store the encrypted file in **public** or **private clouds** such as **Amazon S3, Microsoft Azure, Eucalyptus Walrus** (or internal SAN, NAS drives) while proving compliance to data-security regulations such as **PCI-DSS, HIPAA, EU Directive** etc. The StrongKey CryptoEngine has been in use for nearly a year at a a service provider, encrypting millions of sensitive financial, legal and healthcare documents in a private cloud.

Architected and built a **Public Key Infrastructure (PKI)** for the Central Bank of the United Arab Emirates – the equivalent of the "Federal Reserve Bank" of the UAE. The PKI – using **StrongAuth's PKI Appliances** with FIPS-certified **Hardware Security Modules (HSM)** – will enable strong-authentication for hundreds of member banks in the country to communicate securely with the CBUAE's portal.

Architected and built a **Public Key Infrastructure (PKI)** for a billion-dollar "defense-contractor" to enable Secure Multipurpose Internet Mail Extensions (S/MIME) e-mail for digitally signing and sending/receiving encrypted e-mail with US federal agencies.

Architected and built an appliance – the **StrongKey Lite Encryption System (SKLES)** – for assisting customers with compliance to regulations such as **PCI-DSS**. The SKLES appliance incorporates encryption, tokenization, key-management and a cryptographic hardware module (either a **Trusted Platform Module (TPM)** or an **HSM** – within it. Dozens of SKLES appliances have been sold to customers all over the world.

Designed and wrote the specification for the **eNotarization Markup Language (ENML)** for the **OASIS LegalXML eNotarization Technical Committee**. ENML is expected to move paper-based notarization processes to computer-based electronic notarization, and uses **XMLSignature** as the underlying signing protocol for security. It supports the use of symmetric and asymmetric cryptographic keys for eNotarizing documents.

Architected and built a **Public Key Infrastructure (PKI)** for a US-based medical devices company to embed digital certificates into three components of their new product. Public-key cryptography will be used to prevent counterfeiting of their products, by enabling strong authentication between the components while also providing message confidentiality and data-integrity between components. The PKI is designed to issue millions of digital certificates; it is also expected to be used for standard corporate uses such as smartcard-logon, VPN authentication, signed and encrypted e-mail and encryption of sensitive medical data.

Designed and wrote the cryptography modules for a leading e-commerce platform vendor that hosts 250 e-commerce sites, to enable secure access to the RDBMS and encryption key-management for protecting Credit Card Numbers, as part of their PCI-DSS compliance effort.

Architected and built two PKI's: one based on **Elliptic Curve Cryptography (ECC)** and the other on RSA for a Digital Rights Management (DRM) company. Digital certificates issued from these PKI's are anticipated to be embedded into millions of consumer devices. The PKI's were built using **EJBCA**, **MySQL**, **JBoss** on Windows. **Ncipher**'s hardware security modules were used to protect the cryptographic keys.

Architected and developed an open-source software utility (**CSRTool**) for generating **RSA** and **ECDSA** cryptographic key-pairs, Certificate Signing Requests and then combining the CSR's with the private-

keys to create **PKCS12** files that can be imported into any application that supported import of digital certificates. The utility was written in Java using the **BouncyCastle** JCE provider.

Architected and developed a **Symmetric Key Management System** product (**StrongKey – www.strongkey.org)** to manage encryption keys across the enterprise. The SKMS provides application-independent, platform-independent and database-independent symmetric encryption key-management services using the following components: **JAXB**, **Web Services Security (WSS)**, **XML Signature**, **XML Encryption**, **XPath**, **MySQL, J2EE, SunJCE**, **SunPKCS11** and **PKCS11** libraries from **FIPS 140-2** certified **smartcard** and **Hardware Security Module (HSM)** vendors. The protocol within StrongKey – **Symmetric Key Services Markup Language (SKSML)** – was donated to **OASIS** on a royalty-free basis, for standardization.

Architected and built the security infrastructure, including a PKI, for this startup, consisting of **Sun servers, Solaris9, SunScreen firewall, SunONE servers (Web, Directory, Application, Messaging & Certificate Server), nCipher HSMs, SSH, TripWire, Oracle 9i Database, Oracle 9i Application Server, Windows 2000 Server, Active Directory, IIS, Apache and Red Hat Linux** to support Solaris, Windows and Linux desktops for security operations. Created security policies, procedures, Certificate Policy, Certification Practices Statement & certificate life-cycle procedures for an internal PKI.

Architected and built a scalable, secure, multi-tier J2EE web-application to help companies manage their compliance effort to various Data Privacy laws. The application uses **Jakarta Struts, Log4J, JSTL, CMP EJB, MySQL, Oracle, LDAP, SunONE Application Server** using **certificate-based authentication** and **role-based authorization** for strong authentication. This 4-tiered application runs on Solaris, Linux or Windows and is the only commercial software that does not use UserID/Passwords for access control.

Provided consulting services to **Inovant, Inc. (VISA)** to define certificate life-cycle procedures, and define detailed architectural elements for Visa's US-based PKI deployment to support 50,000+ partners. Also developed a prototype Jakarta Struts-based application for Business Risk Management, to serve as a model for the next phase of development.

Designed and built a worldwide PKI for **Pfizer, Inc.** to support 120,000+ employees to receive digital certificates on their JavaCard smartcards. Technology used was **Microsoft CA, nCipher and GemPlus** smartcards. Business applications that would use this technology were for i) authentication to a Nortel VPN; 2) Windows logon; 3) digitally signed New Drug Applications to the Food & Drug Administration, etc.

Assisted with trouble-shooting a 10,000-seat PKI for a global package delivery company. Customer was running a Windows-based **iPlanet CMS**-based PKI.

SunIT, Sun Microsystems, Inc., Palo Alto, California

PROGRAM MANAGER – SunPKI, May 1999 to June 2001

Responsible for the deployment of a worldwide **Public Key Infrastructure** for Sun to provide employees and partners with Digital Certificates on JavaCards. Using many Sun, iPlanet & third-party products (**SunCluster, Certificate Management System, Directory Server, Web Server, Personal Security Manager, Signtool, nCipher, Chrysalis-ITS, iButtons, Valicert**) with public key technology, the PKI supports next-generation security services to enable secure electronic commerce, through:

- Significantly better authentication using certificate-based authentication, as opposed to userids and passwords
- Confidentiality for business transactions, through the use of encryption (with key-escrow)
- Data integrity for business transactions and software objects, through the use of digital signatures
- Proof of origin & integrity for downloaded software objects, through the use of digital signatures

My responsibilities included deploying the infrastructure in three data centers worldwide, with the attendant business and technical operations to support it. The SunPKI has recently gone into

production, and has started issuing certificates for web-servers and object-signing. Employees will receive their digital certificates with their new JavaCard badges in the second phase of this program, in late 2001. I am currently working on encouraging Sun Engineering organizations to digitally sign all software products and patches, to increase the level of trust and assurance of such software to customers.

Professional Services, Sun Microsystems, Inc., Santa Clara, California

PRACTICE MANAGER, January 1999 to April 1999

In this role, within the professional consulting services arm of Sun Microsystems, I was responsible for the IT Consulting Practice in the Western Area territory of the US. In line with this function, I was responsible for:

- Creating, selling and delivering on programs to provide specialized services - **Server Consolidation, Clusters**
- The successful startup of this business and its growth
- Sales meetings with CIO's and IT management to qualify opportunities
- Presentations on Professional Services to large customer audiences on our service portfolio
- Assessing risks on projects and how they may be mitigated

AREA TECHNOLOGY MANAGER, March 1997 to April 1999

In addition to the Practice Manager role, as the senior-most technologist in the Western Area, I was also responsible for the hiring, growth and nurturing of our primary assets - the technical staff of Sun Professional Services. In line with this role, my responsibilities included:

- Growing the technical organization, from 15 to over 40 in this period
- Focusing and directing the services that this territory provided its customers, to be aligned with Sun's core competencies
- Raising the visibility of Sun & its PS organization by presenting at technical seminars at various trade shows
- Ensuring that the territory was trained and ready to provide technical consulting services, to our customers
- Determining technical sales strategies on different opportunities

IT ARCHITECT, March 1995 to March 1997

As an IT Architect within the Sun Professional Services I was responsible for many aspects of large and complex technical projects for our customers. Starting from initial sales contact for the purposes of qualifying the project, negotiating technical terms for the delivery of the project, preparing Statements of Work to accomplish the customers' objectives, estimating costs and time estimates, to architecting the solution, managing technical resources for the delivery, tracking activities against a technical project plan, and documenting the results. Some of these projects included:

- Creating a new IT architecture for a multinational Transportation company to support their distributed computing vision for 10,000+ desktops in over 200 branches from 2 centralized Data Centers
- Managing the effort to port a quarter-million line, mission-critical software program for a multinational Telecommunications company, from SunOS to Solaris
- Creating a new IT architecture for an international medical technology firm to support secure computing activities across different geographies in the world
- Migrating Oracle ERP applications from HP's MPE operating system to Solaris, for a large Software company
- Server Consolidation for a large Insurance company

Citibank, New York, New York

VICE-PRESIDENT, May 1994 to March 1995

Managed the UNIX and Database Infrastructure group within the UNIX Data Center of Citibank. My responsibilities were to establish a UNIX environment that embodied the best practices of system management, with efficient processes to support production applications of the bank. Chief amongst these were to establish a three-tiered hardware architecture comprising of a Database Tier - consisting of Oracle Parallel Server and Sybase with Replication Server, an Applications Tier - consisting of Applications, NIS+, Lotus Notes, DCE, Encina and other middleware services, and the Presentation Tier primarily consisting of Window-based applications. I was also responsible for establishing standard Data Center processes such as Security & Change Management for the UNIX environment.

BASF Corporation, Parsippany, New Jersey

SENIOR STAFF SPECIALIST, November 1991 to May 1994

I worked as part of a team that served as internal technology consultants to application development groups. My responsibilities were to provide technical guidance on projects that were attempting to develop client-server applications using, primarily, one or more of the following technologies: **UNIX, Oracle RDBMS (Version 7 and 6) & Tools, Oracle CASE, TCP/IP, RPC and/or Socket-level programming, Novell Netware, Windows, X-Windows, Korn Shell, C and C++ Programming, Booch Methodology and Object Modeling Technique.** I made recommendations for specific technologies, architectures and implementation strategies for the projects that I worked on.

New York Life Insurance Company, New York, New York

PROJECT MANAGER, June 1990 to October 1991

As part of a 5-year Information Systems & Services Department project to establish a distributed systems architecture that was to connect over 200 offices together in one Wide Area Network, I managed the Workstation and LAN Server sub-projects to research and recommend the optimal workstations, servers, operating systems, network topology that was to be implemented in the operational environment.

Port Authority of New York and New Jersey, New York, New York

SENIOR SYSTEMS DESIGNER, June 1986 to May 1990

As a member of the Client Services Division of the MIS department, I was responsible for the analysis, design, development and implementation of stand-alone, multi-user and networked systems, working with UNIX, SunOS and Oracle RDBMS.

Conducted analyses of Customers' business problems using Structured Analysis & Design methodology, and provided them with viable and appropriate computing solutions to these problems. Also responsible for the deployment of UNIX for multi-user and networked systems, for commercial applications. Supervised the work of consultants on multiple projects to administer UNIX networks, develop Oracle applications and train users to use in-house developed applications. Some notable projects included:

- Personnel Requisition Tracking System for the HR department to track new hire requisitions;
- Absence Control System for the Tunnels, Bridges & Terminals Dept. to track employee absences;
- Applicant Tracking System for the HR department to track new hires;
- World Trade Institute Database for the World Trade Department to track student registration;
- Port Sales Tracking for the Ports Department to track sales activities

Papers & Seminars

Mainframe reports through E-mail - SUG Conference, San Jose, November 1993
Network Information Services+ - UNIX World, 1994, UNIX Review, 1994
Pretty Good Privacy - UNIX Review, February 1994
Network Information Services+ - Systems Administration Expo, New York, 1994
Pretty Good Privacy - Systems Administration Expo, New York, 1994
Introduction to Java - PC Expo, New York, 1996, 1997, 1998, Network Expo, Dallas, 1996
Network Identity Management Systems - The Final Architecture - Digital ID World, June 2002
Blueprint for dealing with SB 1386 – The ISSA Journal, May 2003
Blueprint for dealing with SB 1386 (Web Seminar) – The ITAA, June 2003
Building a successful PKI – The ISSA Journal, September 2004
Access Control chapter in a book published by the American Bar Association (ABA) – April 2006
Symmetric Key Management Systems (SKMS) – ISACA, San Francisco, September 2006
Enterprise Key Management Infrastructure (EKMI) – OASIS Adoption Forum, November 2006
Enterprise Key Management Infrastructure (EKMI) – SDForum, Palo Alto, January 2007
Symmetric Key Management Systems (SKMS) – The ISSA Journal, February 2007
EKMI – Understanding them before Auditing them – ISACA International, Singapore, July 2007
Enterprise Key Management Infrastructure (EKMI) – ABA – ST-ISC, San Francisco, August 2007
Enterprise Key Management Infrastructure (EKMI) – ISSE 2007, Warsaw, Poland, September 2007
Enterprise Key Management Infrastructure (EKMI) – Burton Group Catalyst, Barcelona, Spain, October 2007
Enterprise Key Management Infrastructure (EKMI) Workshop – ISACA, Hyderabad, India, Nov 2007
Enterprise Key Management Infrastructure (EKMI) Workshop – ISACA, Singapore, November 2007
Enterprise Key Management Infrastructure (EKMI) Workshop – ISACA, San Francisco, Nov 2007
Service Oriented Architecture (SOA) Data Security Workshop – Aachen, Germany, February 2008
Securing the Core with an EKMI – IDtrust Symposium 2008, Gaithersburg, Maryland, March 2008
Identity Protection Factor (IPF) – IDtrust Symposium 2008, Gaithersburg, Maryland, March 2008
Securing data with SOA - OASIS Open Standards 2008 – Santa Clara, April 2008
Data Protection for Companies – American Bar Association SciTech Journal, Summer 2008
Identity Protection Factor (IPF) – Metricon 3.0 (USENIX), San Jose, California, August 2008
Symmetric Key Services Markup Language – ISSE/SECURE 2008, Madrid, Spain, November 2008
Data Protection for Companies – American Bar Association GPSolo Magazine, March 2009
Security 2.0 – an approach to EKMI – CTST 2009, New Orleans, Louisiana, May 2009
StrongKey – Open-source Symmetric Key Management System – NIST Key Management Workshop, Gaithersburg, MD, June 2009
Regulatory Compliant Cloud Computing – OWASP, Boston Massachusetts, May 2011