Information Risk Assessment

This bouquet of Risk Assessment services takes a 360° view of the business, technology and processes through the following offerings :

Business Risk Assessment

- Identification of Business Processes
- Identification of Input/Output Parameters
- Creation of Information Asset Register for processes
- Creation of Business Process v/s Service Dependency Matrix

As-Is Review

- Review of existing procedures and policies
- Gap Analysis vis-à-vis ISO27001 Controls

Information Asset Profiling

- Identification of Asset
- Profile of asset will contain
- Process the asset facilitates
- Format
- Attributes
- Criticality of the asset
- Storage and underlying predecessors

Vulnerability Assessment

Vulnerability Assessment is carried out from inside the network and will cover the following:

- Port scan
- Web server vulnerabilities
- Denial of Service
- FTP related flaws
- Remote shell
- Device Specific flaws
- Telnet Vulnerabilities
- Finger abuses, ICMP flaws
- Application Specific flaws
- Window file structure permission
- Password checks
- Remote file access
- RPC related flaws
- Useless services
- SNMP related flaws
- Windows specific flaws
- SMTP & POP Problems
- Remote privileged access
- Database Vulnerabilities

Attack & Penetration Testing

This assessment checks the possibility of someone (valid or invalid, trusted or untrusted, privileged or unprivileged) situated anywhere on the external network who can gain access by any means (internet leased line, modem, RAS or public net points) to private and presumed secure areas of the target network.

In this test, CyberQ conducts a security analysis on the devices/ servers configured with public IP Addresses but not limited to Servers, Routers, Firewall, Switches, Intrusion Detection Device, Intrusion Prevention device, Proxy Servers etc.

This test is done through an intelligent combination of tools and manual methods and covers the following areas

- Port Scanning
- Services scanning
- Protocol analysis
- Denial of Service
- Buffer overflow
- Operating system loopholes
- MSN & Other Chat services vulnerabilities
- SMTP encapsulation
- WWW content bypassing
- Vulnerability identifications
- Password guessing & cracking

Review of Network Security Assessment / Architecture

- CyberQ will conduct a detailed analysis of all the network assets.
- Review of Network Architecture will cover the following :-
    - Remote and external access methods
    - Remote administration of critical devices
    - Network Exposure to unauthorized access from Internet
    - Confidentiality / Integrity of Incoming / Outgoing data to Intranet / Internet
    - DOS (Denial of Services) attacks on network resources

Application Security Assessment

- While testing the application based on OWASP and SANS vulnerabilities, CyberQ checks for, but not be limited to, the following:
    - Invalidated inputs
    - Broken Access control
    - Improper error handling.
    - Denial of service attack
    - Remote File inclusion
    - Cross Site Request Forgery (CSRF)
    - Injection Flaws

- Broken Account and Session Management
- Buffer Overflow
- Cross-site scripting (also referred to as XSS)

Public Key Infrastructure (PKI)

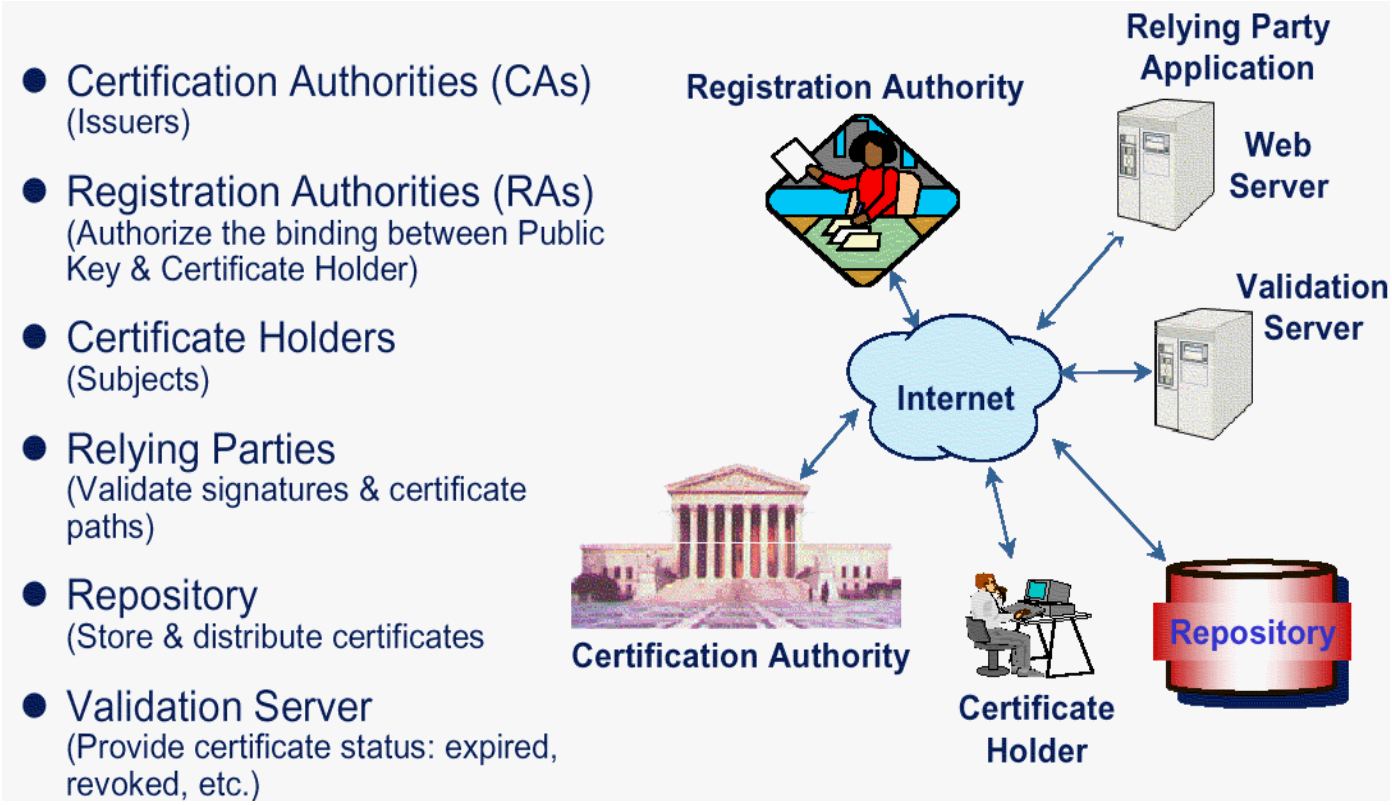
Introduction

Public key infrastructure (PKI) is cryptography-based technology used to secure electronic processes and transmission.

The basic idea is that sensitive data is protected through encryption. Each end-user device has encryption software and two keys: a public key for distribution to other users, and a private key, which is kept and protected by the owner.

PKI enables the centralized creation, distribution, tracking and revocation of keys.

Components of PKI:



To get a certificate, a user sends a request to a designated registration authority, which verifies the user's identity and tells the certificate authority to issue the certificate.

PKI Audits

In India, the Information Technology Act was passed in the year 2000 and further amended in 2008. The IT Act provides legal recognition for electronic transactions. The Controller of Certifying Authorities (CCA) is the root CA. CCA establishes a methodology for auditing CAs

. Any company wishing to become a CA has to apply to the CCA. The CCA has a defined methodology for auditing the company. Based on the audit, the company is granted a license to operate as a CA.

CyberQ is one of the Empanelled Auditors of CCA, qualified to perform Pre-operative audits for CAs, as well as routine Annual CA and RA audits.