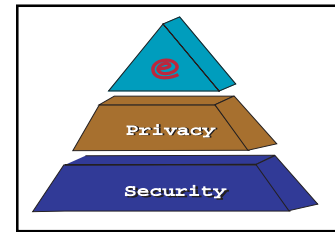# IBM Global Services
e-business Security and Privacy Services
PKI Consulting and Integration Services

## IBM Global Services: Worldwide coverage for consulting, design and integration services

The challenge... Business transactions on the Internet require security services to parallel the trust enabling safeguards of the physical world. And while Public Key Infrastructures (PKI) are emerging as the primary component for enabling new trust models in e-business, they are complex, not easy to implement, and have far ranging impacts on both IT and business practices.

The solution... IBM Global Services End to End PKI Capabilities

IBM Global Services™ has PKI capabilities that can be customized to meet clients' needs. IBM's capabilities for planning, designing, implementing, outsourcing and assessing PKIs include:

PKI Plan

- **PKI Workshop -** helps business and IT decision makers understand PKI technology, policy and implementation considerations; and formulate a preliminary strategy and action plan for applying PKI to their business.

- **PKI Strategy -** establishes a PKI strategy that identifies the roles of the client, its business partners and customers; the applications that will be supported; the registration and trust models, the level of security, and a roll-out plan.

- **PKI Readiness Assessment –** assesses the client's capabilities for utilizing and implementing a PKI, with recommendations for steps the client should take to be PKI ready, including an estimate of the costs.

- **PKI Value –** identifies the value of implementing the client's PKI strategy, for use by the client in their PKI businesscase.
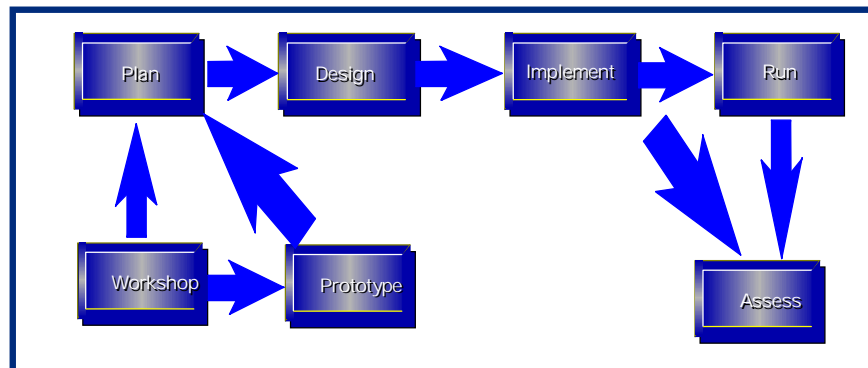
IBM Global Services will provide customized PKI consulting and integration services that address specific business requirements as well as end-to-end infrastructure and application development and integration

- **PKI Requirements –** establishes the business requirements (e.g., applications, services, interoperability, naming, trust, process, security, legal, contractual, workload, performance, RAS, recovery, scalability and record-keeping) for the client's PKI as they relate to the client's current and future business needs, including specification of key security processes.

- **PKI Policy –** establishes the policy for identity assurance for issuing certificates, the security policy for supported applications, and the requirements for certificate policies, Certification Practice Statements and policy mangement.

- **Conceptual PKI Architecture –** creates a high level conceptual architecture for PKI solutions that satisfies the client's PKI requirements and PKI policy, identifying the PKI components, trust model and design principles.

- **Functional PKI Architecture –** creates a functional PKI architecture that builds upon the conceptual PKI architecture and defines the required PKI functions and relationships between those functions, including the PKI and certificate management life cycle services, subject naming, the registration and trust models, trust

infrastructure, assurance levels, certificate policies, CRL issuance, interoperability requirements, and record keeping and protection.

PKI Design

- **PKI Product Selection –** analyzes client's PKI requirements and functional PKI architecture against industry solutions, covering both products and services, to enable the client to select the technology that best fits their needs.

- **Site Selection and Facility Design –** helps client evaluate potential site locations and provides secure and available facilities design, consulting and deployment.

- **Process Development –** describes the processes needed to support the PKI (e.g., registration, revocation, record keeping, CA key generation) as well as those for integration into other IT processes (e.g., backup and recovery, system management, help desk), and provides recommendations for process automation**.**

- **Component PKI Architecture –** creates a component PKI architecture that builds upon the functional PKI architecture and defines the technologies, standards, interfaces and

IBM Global Services
e-business Security and Privacy Services
PKI Consulting and Integration Services

selected products that satisfies the client's requirements, strategy and PKI policy.

- **PKI Certification Practices** – creates the technical portions of the Certification Practice Statements and certificate policies for an organization's Certification Authorities.
- **Implementation Plan** – plans the next steps in implementing the PKI.

PKI Implementation

- **System Integration -** integrates PKI and IT components so the business' needs are met.
- **Application Development** – develops custom PKI enabled applications as well as applications needed for PKI system management and registration.
- **Operational Procedures** – defines the operational procedures for the roles administering some part of the client's PKI (e.g., system administrators, system operators, CA administrators, directory administrators, registration authorities, security officers, policy managers, and help desk personnel).
- **PKI Test Plan** – develops a comprehensive test plan for a PKI prototype, encompassing all aspects of the planned deployment: hardware, PKI applications, processes, policies and system management. Plans unit tests to test all functions and processes, load tests to test reliability and performance, and system problem tests to test system management and recovery for responding to system problems.
- **PKI Training** – trains client on how to manage and run the PKI, and optionally educates client's PKI users about PKI and their responsibilities.
- **PKI Prototype** – helps client implement a non-production prototype using the component PKI architecture and security practices with a small number of subscribers and relying parties.

- **PKI Test** –conducts the PKI test plan on the prototype.
- **PKI Pilot** – helps client run a PKI pilot with the production system and a small number of subscribers and relying parties for testing the total solution and identifying major problems before opening up the service for general production.
- **PKI Production** – provides client with assistance in resolving problems for a specified number of days after the production cut over.

PKI Outsourcing

- **IBM Outsourcing** - runs PKI services at IBM sites for clients who wish to outsource their PKI. Such an arrangement allows clients to use local Registration Authorities for administering certificate registration requests by their customers.
- **Third Party Outsourcing** - Helps clients who need certificate services from a trusted Certification Authority.

PKI Assessments

- **CPS Compliance Assessment** – assesses the client's PKI security practices against the procedures described in the client's certification practice statement(s).
- **System Security Assessment** – assesses the security of the client's PKI servers and administrators.
- **Network Security Assessment** – assesses the security of the client's network used by PKI components, especially Certification Authorities and Directories.
- **Site Security Assessment** – conducts an in-depth review of the client's security controls and processes at the site where
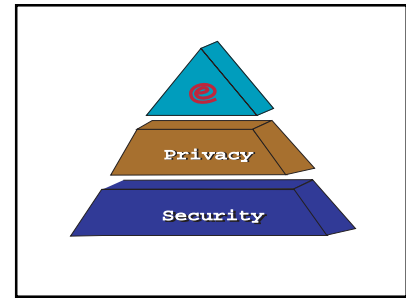
Certification Authorities and other security-sensitive PKI components are managed.
- **Security Process Assessment** – conducts an in-depth review of the client's security processes used for administering the PKI.
- **Ethical Hacking** – tests client's Certification Authorities and other security-sensitive PKI components by trying to break into client's systems or facilities.

Contact your IBM representative to discuss your specific needs. Additional information can be found at our web site