VeriSign Public Key Infrastructure Overview

Digital Certificates and PKI

Public Key Infrastructure

- **The infrastructure needed to issue and maintain Digital Certificates**

  A PKI (public key infrastructure) enables users of a public network such as the Internet to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

- **Most of it lives in our secure datacenters**

  VeriSign Services for government authentication have been certified to the highest technical and policy standards of the United States Government and are approved for deployment to Federal, state, and local agencies and government contractors.

- **Your Data is Secure**

  VeriSign undergoes an external, third-party operational audit on an annual basis The annual audit provides our customers with outside, independent confirmation that VeriSign complies with its rigorous information system security requirements as stated in our Certificate Policies (CP), Certification Practice Statement (CPS) and Security and Audit Requirements (SAR) Guide.

VeriSign®

So, Why Use PKI?

- PKI was selected for NSTS and is the ***only*** technology that provides all of the essential security services needed for establishing trust in on-line electronic transactions: confidentiality, integrity, identity authentication and non-repudiation

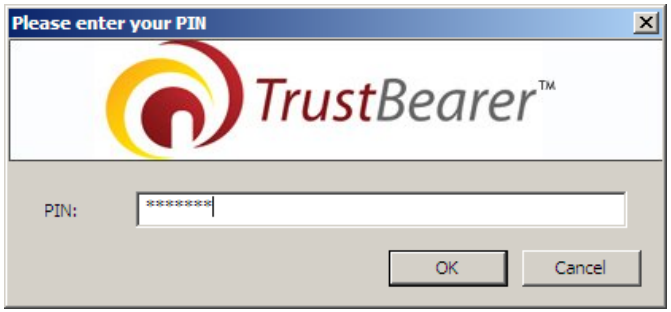
- PKI enables trusted transactions between two unrelated parties

- PKI is robust, scalable, the identity credentials are not easily forged, spoofed, copied or broken

Strong Authentication

+ Strong Authentication is used to secure activity in enterprises and other organizations, like the government

+ For NSTS, Strong Authentication is comprised of:



‘**Something you know**’, such as a PIN

‘**Something you have**’, such as a smart card

NRC Credentialing Process

Step 2
Online application is reviewed and approved

Step 3
A paper identity proofing packet is mailed to the applicant

Step 4
The paper packet is completed by the applicant, notarized, and mailed back

Step 5
The paper packet and online application are reviewed, anomalies are resolved with the applicant, employment is verified and the enrollment is approved

Step 6
A smart card and reader are mailed to the applicant

Step 7
Reader is installed and used to download the applicant's certificate to the smart card