Quick Reference Guide

Understanding the Two Factor Authentication requirement for CJIS.

This quick reference guide explains:

Two Factor Authentication
Identity Assurance (PKI)

If you have any questions, please contact sales@txsystems.com.

Two Factor Authentication is

a term that is used often but not always understood. In order to understand two factor authentication, you must first know exactly what “a factor” is.

Three Main Factors:

1) Something you have – a physical object like a building access card
2) Something you know – something in your head, like a password or pin
3) Something you are – something that is part of you, like a fingerprint or iris scan




Two factor authentication is simply the implementation of any two of these factors before a user can logon to a system.

Products:

Identity Assurance;

Public Key Infrastructure (PKI)

PKI is the same security methodology used by the DOD, DHS, NSA, DOT, and FBI to issue their secured ID badges known as CAC, PIV and TWIC Cards. In a PKI deployment, users authenticate with a contact smart card plus a pin code to authenticate back to Active Directory or secure websites. In addition to two factor authentication, digital certificates can also be stored on the PKI card for digital signing of documents and email encryption.



Inside of this chip are a few different digital certificates that allow the user to do different things. Each certificate has a different function. The most common certificates are for:

1) Secure Windows Logon
2) Secure Application Logon
3) Secure VPN Logon
4) Digital Signature for documents, email, code or data packages
5) Email Encryption and Decryption for secure email exchanges

Products: