Quick Reference Guide

Passwords can be lost or stolen during a data breach or left in unsafe places such as under the keyboard or taped to the computer.

This quick reference guide explains:

Two Factor Authentication
Identity Assurance (PKI)
Strong Authentication

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 a security method for storing digital credentials onto a smart card. This is the same technology that the US Government uses to validate the identities of service men and women in the military and in Government agencies. This is the most secure way we know of validating the Identity of a person in the digital world.



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:

Sample idOnDemand SmartID

Strong Authentication is when we add a more complex layer of authentication onto traditional logon. Most of the time people logon to a domain or VPN with a username and password. By adding a more secure method of authentication, you are making it harder for intruders to access your secure systems. Strong Authentication is traditionally used most when people are trying to login to a network remotely, when they are on the road or outside of the building.

There are many different Strong Authentication devices and methods in the world. Some of the most common devices in use are:

1) One Time Password (OTP) devices
2) Smart Tokens
3) Soft Tokens for Laptops
4) Soft Tokens on Smart Phones

Products:

About Us

Tx Systems is a Value Add Distributor of Strong Authentication products for Identity Assurance and Access Management. We have been in business since 2001 and have a deep knowledge of the security products surrounding building access control and network logon, whether inside or outside of the firewall.

In addition to our security solutions suite, we are also the leading distributor of smart card readers being sold into the Federal Government for the Common Access Card (CAC) used by the DOD, DHS, and NSA, as well as the PIV card used by the leading Government contractors. Our decade of working with these cards has given us a unique perspective on security, specifically concerning smart cards. As technology progresses and the smart card evolves, you can count on Tx Systems to be well versed in all aspects of security surrounding the validation of identity in the growing digital world.

Our in house engineering staff makes it possible for us to assist our customers and partners in security installations from beginning to end. Tx Systems is here to assist in every step of the opportunity from presales consultation, to solution recommendation, until the finally deployment is done. We are truly happy to be able to assist with your security needs, no matter the capacity.

We hope to speak with you soon.

Best Regards,

Tx Systems Staff

Jason Wimp
President, Founder

Casey West
Vice President of Sales and Business Development

Alex Howard
Head of Engineering

Eric Gregg
Enterprise Sales Manager

Jared Pabis
Government Sales Manager

TX Systems

6242 Ferris Square • San Diego, CA 92121 • Tel: 858-622-2004 • www.txsystems.com