Cygnacom Solutions

The Federal Cyber *Security Sprint* is Underway

Ready, Set, Go !

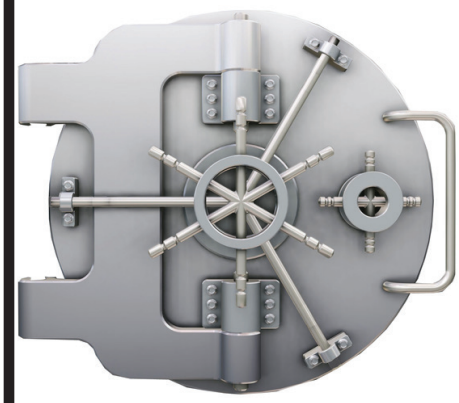
Cygnacom has the expertise to support your smart card authentication program

"65% of Federal civilian security incidents were related, or could have been prevented by Strong Authentication implementation" [1]

Your PIV Cards are the Key to Preventing:

- Malicious network activity
- Unauthorized access
- Phishing attacks
- Loss/misuse of government data & equipment
- And many other attacks

Cygnacom Provides The Strongest Lock:



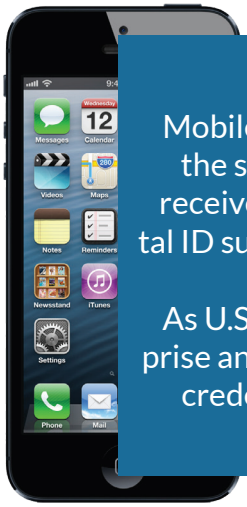
- As an Entrust Datacard company, Cygnacom is the major provider of SSP certificates for the US Federal government
- Cygnacom built and operates the first datacenter for the Entrust Managed Service, providing certificates & PIV cards for the US Access Program, as well as cloud-based PKI, card-issuance and authentication services
- As an Entrust Datacard company, Cygnacom is the best choice for deploying Entrust PKI and digital certificate consulting services
- Since 1994 Cygnacom Professional Services has provided IT security consulting services to every government agency
- 100% of our Professional Services team holds a minimum of top secret clearance

Don't be Tomorrow's Headline

703-270-3500 ps@cygnacom.com

Cygnacom's Smart Card Authentication
Rapid Deployment Package

- A dedicated senior Cygnacom senior security architect will be assigned and a technical workshop will be scheduled. During the technical workshop the senior security architect will:
  - ☑ Interview key personnel to better understand the environment, current challenges, and implementation requirements
  - ☑ Identify components that may have a direct impact on the smart card logon deployment
  - ☑ Define the approach and strategy that may be leveraged to successfully deploy smart card logon and mobile device integration.
- Based on the discussion during the technical workshop, the security architect will prepare a corresponding Smart Card Deployment Strategy document. The document will provide recommendations based on customer's unique requirements to achieve smart card login requirements and comply with HSPD-12 directives.
- The security architect will review the Smart Card Deployment Strategy document with customer and agree upon next steps.
- Based on the Smart Card Deployment Strategy document and the mutually agreed upon next steps, a Cygnacom Project Manager will prepare a comprehensive project plan to assist customer in achieving the deployment.



It's More Than a Trend

Mobile devices are becoming the new enterprise desktop. But mobile devices require the same security considerations to access corporate intranets or securely send and receive email. Deriving a credential for a mobile device based on a user's existing digital ID such as a government-issued PIV credential is a great benefit to an organization's security plans.

As U.S. federal agencies continue to investigate their options to bring standard enterprise and mission-critical applications securely to employees' mobile devices, a derived credential is a great choice to simplify the processs. Cygnacom can help you support and solve some of the most commonly requested use cases.

Cygnacom Provides Expert Consulting In:

- Multi factor authentication solutions
- Mobile device credentials
- Derived credentials
- Strong data data protection solutions

[1] Annual Report to Congress: Federal Information Security Management Act Office of Management and Budget, February 27, 2015.

Cygnacom is Ready To Help

703-270-3500 ps@cygnacom.com