Solution Brief

Thales TCT Multi-Factor Authentication (MFA) for Commercial Solutions for Classified (CSfC) for Mobile Access

thalestct.com

THALES
Building a future we can all trust

What is CSfC?

Commercial Solutions for Classified (CSfC) is a program that enables commercial products to be used in layered solutions to protect classified information. This speeds up the deployment timeline so that a solution can be fielded in months, versus years. The program was designed to allow simultaneous use of multiple unclassified commercial off the shelf (COTS) products instead of classified, Type 1 U.S. Government accredited products to secure classified data within government deployments.

CSfC promotes the protection of critical data with layered encryption technologies. A layered encryption approach is most effective when each layer can stand independently relative to their design, implementation, and operational deployment. There are currently four approved CSfC Capability Packages (CP), each of which outlines overall customer solution architecture requirements as well as specific device configurations.

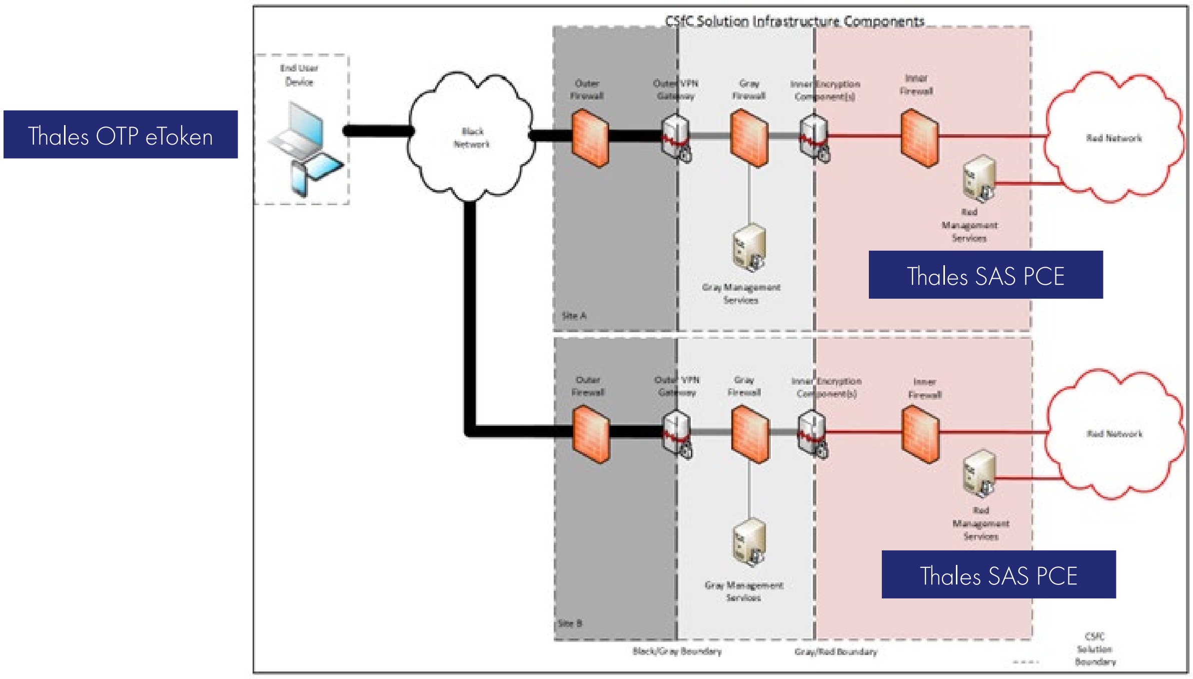
The Role of MFA in CSfC

The CSfC Mobile Access (MA) solution provides mutual device authentication between Outer VPN components and between Inner Encryption components via public key certificates. There are two scenarios within the MA CP for multi-factor (aka two factor) authentication: "User to EUD" and "EUD to Infrastructure." This solution brief will focus on the integration of Thales MFA into CSfC Mobile Access solutions.

Thales TCT Products Address CSfC MFA Requirements for Mobile Access

Both the User to EUD and the EUD to Infrastructure MFA requirements summarized in sections 4.4.2.1 and 4.4.2.2 of the CP MA describe use of a physically separate token to serve as the "something you have" factor of the MFA solution. Listed as objective requirements in v2.5.1 of the MA CP, most approved CSfC solutions have yet to integrate token based MFA in fielded solutions. However, changes in the MA CP to elevate the MFA requirement to the threshold level will necessitate integration of One Time Password (OTP) token based MFA.

Thales OTP authenticator devices teamed with the Thales SafeNet Authentication Service (SAS) PCE Identity Provider (IDP) application provide a mature and well tested solution to directly address these CSfC requirements. The Thales MFA solution meets all 12 requirements detailed in Table 28: EUD to Infrastructure Multi Factor Authentication Requirements. Similarly, the Thales MFA solution meets all of the requirements allocated to OTP MFA tokens in Table 29: User to EUD MFA Requirements. The following diagram illustrates how Thales OTP tokens integrate at the EUD (as an EUD or VPN authenticator) and the corresponding SAS PCE server resides in the management network.



Ref. Overview of Mobile Access Solution, Figure 1

OTP Authenticators

- **Approved** — Fielded in several U.S. Federal agencies
- **Standards Compliant** — Fully OATH Compliant (TOTP & HOTP)
- **CSfC Compliant** — Meets CSfC Mobile Access CP MFA requirements (Tables 28 and 29)
- **Effective & Efficient** — Small, reliable, easy to carry & use. One button. No PIN.
- **Secure** — Encrypted seed file delivery
- **Selection** — Various form factors to choose from:

OTP Display Card

eToken PASS

OTP 110

SAS PCE IDP

- **Easy & Secure**
  - On-Premises Auth platform
  - Simple management interface
  - Robust API
  - Comprehensive degree of automation
- **Compliant** — FIPS 140
- **Mature** — 200 out of the box pre-tested configurations

Proven Integrations

As part of the Thales TCT Technology Partner Program, Thales TCT provides extensive and on-going technical integration support. The Thales portfolio of MFA OTP authenticators and SAS PCE management server have an extensive list of proven integrations for both end user device authentication and VPN authentication. The Thales TCT MFA authentication solution can be integrated with the most widely deployed VPN solutions to meet the MA CP EUD to Infrastructure MFA requirements.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct.com

©2024 SafeNet Assured Technologies, LLC 5.1.24