

The Thales logo is displayed in a bold, white, sans-serif font. The letter 'A' is stylized with a blue dot above it. The background of the slide features a blurred office scene with two people, a woman on the left wearing a headset and a man on the right, both looking towards the right. A large blue geometric shape, consisting of a triangle and a circle, is overlaid on the right side of the image.

THALES

STA Survival Kit

Jan Snowball 27th March 2020

Comprehensive list of resources to use for STA campaign
Contains some Partner-Sensitive materials

Version 1.0

CONTENTS

- [Overview](#)
- [Fact Sheet](#)
- [Brochures](#)
- [Solution Briefs](#)
- [Product Briefs](#)
- [White Papers](#)
- [Reports](#)
- [Case Studies](#)
- [Webinars](#)
- [Videos](#)
- [Cheat Sheets](#)
- [Competitive](#)
- [Tools](#)

THALES





Discover the Benefits of Using a Policy Driven **Smart Single Sign-On** Versus a **Simple Single Sign-On**

▲ SIMPLE SSO VS SMART SSO ✓

Feb-20

Security Risk If the SSO credential is compromised, all applications are vulnerable	Secure User benefits from the SSO experience but risk is mitigated by step up authentication only when required
Lack of Visibility Unable to track which apps are being accessed where and when	All Eyes Ability to monitor logs, see who accesses what, when, where and how
Open Access One single access policy for all users and applications	Policy Driven Set access policies per business need, application sensitivity and employee function
Point Authentication User has the same method of authentication to access all services	Universal Authentication Apply the appropriate MFA or contextual authentication method to each login attempt

SafeNet Trusted Access
 • Cloud based
 • Enable cloud transformation security
 • Simplify compliance

THALES

Visit <https://safenet.gemalto.com/access-management/>

4 Reasons To Migrate from your Current Solution to **SafeNet Trusted Access**

Say goodbye to

- 3 year token renewal cycles
- Time consuming management & maintenance
- High costs

Feb-20 V2

Say hello to **SafeNet Trusted Access**

Award-winning Multi-factor Authentication AND Cloud Access Management delivered from one integrated cloud service.

Migrating from your current solution couldn't be easier

Keep your current tokens and servers, while incrementally migrating to a multi-tier, multi-tenant cloud environment as your licenses expire. No need to rip and replace!

- Proven technical migration path**
Use the same technical migration path already used by hundreds of happy customers.
- Simple pricing model**
Pay one simple all-inclusive subscription fee. No three-year token renewal cycles. Just subscribe, and you're done!
- Lower TCO**
Reduce your Total Cost of Operation (TCO) with intuitive management, simple integrations and cloud efficiencies. 100% cloud solution.
- MFA and Access Management in one solution**
Secure all your apps with the best multi-factor solution on the market, and offer trusted access to all your cloud apps with cloud SSO and granular access policies.

Follow us on: Learn more about cloud-based access management powered by award-winning multi-factor authentication safenet.gemalto.com/access-management

SafeNet Trusted Access
 • Cloud based
 • Enable cloud transformation security
 • Simplify compliance

THALES

BREAKING
The Silence of the PAMS
Privileged Access Management

ARE ATTACKS TO PRIVILEGED ACCOUNTS DANGEROUS?

Yes. Attackers who gain control of privileged accounts can have the key to the IT kingdom. They can take over enterprise IT, reset permissions, steal confidential data for fraud, cause reputation damage, and introduce malware and viruses.

DO PAM SOLUTIONS SECURE PRIVILEGED ACCOUNTS?

To a point. A PAM solution can ensure the security of privileged accounts only if the IT admin accessing the solution have the right to do so.

DO ACCESS MANAGEMENT AND MULTI-FACTOR AUTHENTICATION ENHANCE PAM?

Yes. By enforcing the right access policies and strong authentication methods when IT professionals login to the PAM solution, Access Management helps ensure that only the right people reach your resources.

DOES ACCESS MANAGEMENT OFFER USER CONVENIENCE?

Yes. With smart SSO, Access Management lets you step up or down by implementing different access policies and authentication methods for different groups. Need stricter security? Working on-prem? Step up and down according to your security needs, without having to manage endless sets of passwords.

BREAK THE SILENCE AROUND THE VULNERABILITY OF YOUR PAM.

Learn how Access Management and strong authentication can enrich PAM, secure your resources and add user convenience.

SafeNet Trusted Access
 • Cloud based
 • Enable cloud transformation security
 • Simplify compliance

THALES

Visit <https://safenet.gemalto.com/access-management/>



thalescpl.com

THALES

4 Steps to Cloud Access Management

A Practical Step-by-Step Guide to Managing Cloud Access in your Organization

Cloud Access Challenges in the Enterprise

Cloud apps in the enterprise have become mainstream, with 93% of organizations using cloud-based IT services¹. But leveraging cloud-based applications comes with its share of challenges. As organizations embrace cloud apps for their quick time to value and best of breed technology, they are confounded with increasing management and usage complexities.

Password fatigue

Users need to maintain countless usernames and passwords. They are required to authenticate numerous times every day with each application they open, and often resort to security workarounds. This leads to password fatigue—the exhaustion that results from the endless need to create, update and reset passwords for different applications on a daily basis.

Poor security

By default, cloud apps are only protected using weak, static passwords—a reality that jeopardizes the confidentiality of sensitive information and increases the risk of a breach. The majority of worldwide data breaches can be thwarted using strong two-factor authentication².

Complex management

Each new cloud app brought into the enterprise requires management and user-troubleshooting from a different console or admin portal. When a dozen or more apps are used across the business, administration becomes unscalable.

Compliance risk

Proving regulatory compliance requires visibility into access events. IT departments need to know who is accessing what app and when. Furthermore, with sensitive data residing in cloud apps, administrators need to know how users' identities are being verified.

High helpdesk costs

The proliferation of cloud identities and access credentials results in frequent password resets, which account for 20% of an organization's helpdesk costs³.

¹ Source: Spiceworks, Survey: 93 Percent of Organizations Use Cloud-Based IT Services
² Source: Verizon 2016 Data Breach Investigations Report
³ Source: Siftware, Forgotten user passwords - Eliminate the Problem Dramatically Reduce the Cost



4 Steps to Cloud Access Management Guide Book

2

6 Page A4
Sept 19
RMv2



2 Page A4
May 19
v2

thalescpl.com

THALES

SafeNet Access Management and Authentication Solutions

Prevent breaches, secure cloud migration & simplify compliance



Cloud-based applications play a vital role in fulfilling productivity and operational needs in the enterprise. However, as new services are added to an organizations' cloud estate, it becomes more difficult to gain unified visibility into cloud access events, more complex to comply with regulations and more onerous for users to remember multiple credentials. And with cloud applications protected, by default, only with weak static passwords, the risk of a data breach rises.

Thales's award-winning suite of SafeNet Access Management and Authentication solutions allow organizations to effectively manage risk, maintain regulatory compliance, gain visibility into all access events and simplify the login experience for their users.

Utilizing policy-based SSO and universal authentication methods, enterprises can securely move to the cloud while maintaining access controls to all corporate resources, regardless of the device being used.



Prevent breaches

Deter unauthorized access and apply universal authentication methods for all apps

Enable cloud transformation securely

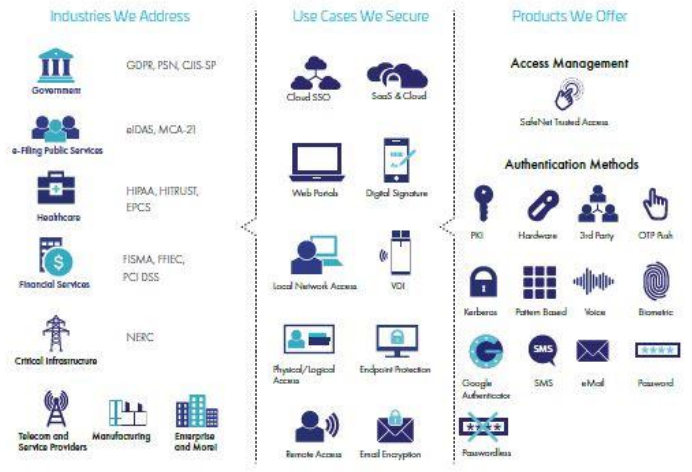
Transform your business and operate securely by applying consistent access policies to all on prem and cloud apps

Simplify the login experience

Make it simple for users to log into multiple apps with cloud SSO, elevating trust only when needed

Simplify compliance

Remain compliant as you grow your environment by setting policies that adapt to new regulations



Standards-based Security

Thales's SafeNet Access Management and Authentication solutions offer unparalleled standards-based security:

- FIPS 140-2 validated software and hardware tokens
- Common Criteria certified hardware tokens
- ISO 27001:2013 accreditation
- AICPA SOC-2 recognition
- DSKPP-secured provisioning of software tokens
- ANSSI certified libraries within software tokens
- Hardware-based root of trust
- Field-programmable tokens



thalescpl.com

Americas - Thales Security Inc. 2060 Junction Ave, San Jose, CA 95134 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalessec.com
 Asia Pacific - Thales Transport & Security (HK) Ltd, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2855 8630 • Fax: +852 2855 8140 • E-mail: asia.sales@thalessecurity.com
 Europe, Middle East, Africa - Meadow Way House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201000 • Fax: +44 (0)1844 208550 • E-mail: enesales@thales-security.com

© Thales - May 2019 - V20B



Customer Handbook

20 Page
10cm x 10cm
Sept 19
ELCv10



Contents

An Introduction	3
Glossary of Access Management Terms	4
Identity and Access Management (IAM)	4
Access Management	5
IDaaS	6
Identity Governance and Administration (IGA)	6
Identity Federation	7
Federated Login	7
Identity Provider	8
SAML	9
WS-Fed	11
Open ID Connect	13
Single Sign-On (SSO)	15
Password Vault	16
Authorization	17
Authentication	17
Context-based Authentication	18
Continuous Authentication	19

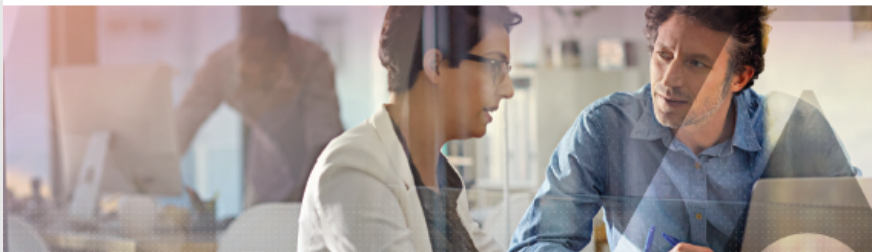


2 Page A4
May 19
BBv1

thalescpl.com

THALES

Matching Risk Policies to User Needs with Cloud Access Management



Whereas traditional Single Sign-On solutions apply a blanket policy to all target resources, access management solutions have emerged to offer the convenience of SSO combined with the fine-grained security offered by customizable access policies.

By applying SSO to target web and cloud applications, while fine-tuning access controls and authentication requirements per specific use-case scenarios, organizations can offer their users frictionless access while remaining protected, compliant and in control.

Fine-Grained SSO Access Security

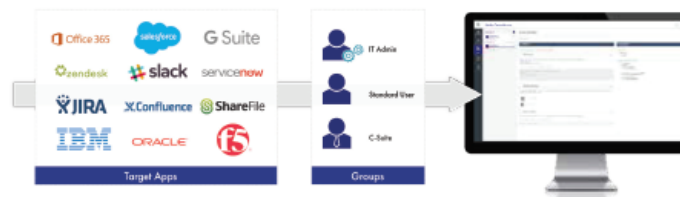
When configuring policies for business critical applications, organizations normally opt for more stringent access controls to elevate the assurance that a user is who they claim to be. The same is true for securing access by privileged users, remote workers, external consultants or contractors and securing access from countries where your organization does not normally do business. These use case scenarios can be easily accommodated using dedicated, fine-grained access policies configured for cloud and webbased services.

Applying elevated Access Controls on Remote Workers

Remote workers logging in outside of the corporate network may require additional authentication factors, as compared to local



workers logging in from the office. To this end, a global policy can be set up, requiring only a domain password for users launching an SSO session from within the office, inside the corporate network. An exception policy can be added to require an additional authentication factor, such as a one-time passcode (OTP), for any user external to the known network, logging in from outside the office. In this way, users logging in from inside the office, log in to the SSO session only with a domain password, and can then easily move from one application to another (unless configured otherwise). Conversely, users logging in from outside the office would be prompted to enter a second factor in the form of an OTP.



Applying elevated Access Controls on Business Critical Applications

Some organizations may wish to offer SSO to most of their applications, while requiring elevated access controls to business critical applications that harbor sensitive data or underlie core infrastructure. Addressing this scenario, IT administrators can set up a policy requiring password-only authentication for users accessing their first app at the start of their day. An exception policy could be added to require additional authentication for users accessing business critical applications. For example, users could be prompted to enter an OTP, or approve a login request pushed to their mobile device.

Applying elevated Access Controls on certain Geographic Locations

Organizations concerned about access to their applications originating from geographic locations where they don't typically do business, can either deny access attempts coming in from identified countries, or they can define more stringent access controls for these access attempts. Configuring specific controls around access attempts originating from these countries, allows organizations to monitor activity originating from certain locales. For example, an exception policy could be set up to require multi-factor authentication each time a single sign on session is started from any of the identified geographies.

Apply elevated Access Controls on External Consultants

Businesses who wish to provide their core internal users an SSO experience, while elevating access controls for external contractors and consultants, can do so by configuring a policy based on this user group, which requires a second authentication factor each time a single sign on session is initiated. In this way, contractors can still enjoy frictionless access to all their applications, while IT can elevate the assurance level around SSO sessions launched by this group of users.

Strategic Value for your Business

SafeNet Trusted Access is a cloud access management service that offers single sign-on secured by granular access policy enforcement.

By enabling IT Administrators to create use-case based policies, SafeNet Trusted Access provides them with flexibility in protecting their organization and sensitive applications without adversely impacting the end users' SSO experience.

Granular exception policies empower IT to increase security on specific applications, geographies or groups of users, while providing a frictionless access journey to core users and use-cases.

By tailoring access policies to the scenario at hand, IT can ensure that policies are as stringent or as lax as required, prompting for no credentials, a single credential or multiple credentials each time a user logs in to an SSO session or an individual app.

To learn more about access management from Thales, visit <https://safenet.gemalto.com/access-management/>, or join a live demo webinar at <https://www.brighttalk.com/webcast/2037/334449>

About SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

Benefits of Scenario-based Access Controls

- Offer the convenience of SSO without sacrificing security
- Require stronger access controls per SSO session or per individual app
- Tailor access policies per application, geography or user group
- Easily meet regulatory mandates by setting up dedicated access policies, e.g. PCI DSS, GDPR, PSN, EPCS etc.
- Configure access policies to be as stringent or lax as required

> thalescpl.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel: +1 888 744 4974 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalessec.com
Asia Pacific – Thales Transport & Security (HQ) B, Unit 4101-3, 41/F, Sunlight Tower, 249 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8341 • E-mail: asia.sales@thales-sec.com
Europe, Middle East, Africa – Thales New House, Long Gardens, Watlington, Oxon OX11 1BB UK • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: www.sales@thales-sec.com

© Thales - May 2020 - BBv1



2 Page A4
MAY19
EHV3

thalescpl.com

THALES

PKI Portfolio Brochure



Thales offers comprehensive public key infrastructure (PKI) access management and authentication management solutions that provide optimal levels of security. Supporting a wide portfolio of SafeNet IDPrime cards and USB tokens, SafeNet access management and authentication solutions ensure the proper security controls are in place to verify the identity of users and enable advanced security applications such as authentication, digital signing and encrypted email on any PC, desktop or mobile device.

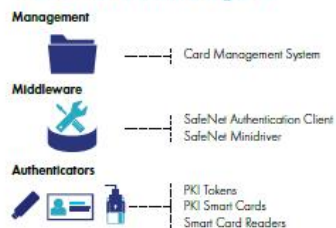
Applicable for a variety of vertical industries.



Thales PKI solutions serve many use cases:



Thales PKI Portfolio at a glance



Management

The need to securely and timely manage users and authenticators is important with any PKI-based deployment. Thales offers the most comprehensive access and authentication management systems management systems to administer, monitor, and manage strong authentication deployments and digital signing across the organization.

Middleware

Thales middleware enables strong authentication operations and the implementation of certificate-based applications such as digital signing, network logon and password management. Because not every organization has the same needs, we have a full middleware client solution, as well as a light-weight minidriver option that is fully integrated on Windows.

Advanced Management Functionality

- SafeNet Authentication Client: Full management solution, providing full local admin and support for advanced card and token management, events and deployment

Light Management Functionality

- SafeNet Minidriver

Authenticators

Thales's broad portfolio of PKI-based authenticators, including SafeNet multi-factor solutions, offers a variety of options including contact cards with a wide choice of card body options and contactless technologies, dual interface cards compatible with NFC and USB tokens and secure storage.

About SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

Authenticators-Form Factors

Gemalto offers a broad range of form factors, allowing customers to address numerous use cases and levels of assurance.



> thalescpl.com <

Americas – Thales Security Inc, 2840 Junction Ave, San Jose, CA 95134 USA • Tel: +1 833 744 4574 or +1 954 838 6200 • Fax: +1 954 838 6211 • E-mail: sales@thalessec.com
Asia Pacific – Thales Transport & Security (HK) Co, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-sec.com
Europe, Middle East, Africa – Thales New York, Long Beach, Maryland, Buckinghamshire HP18 9EJ • Tel: +44 (0)1844 210800 • Fax: +44 (0)1844 210850 • E-mail: www.sales@thales-sec.com

©Thales - MAY 2019 - EHV3



Contents

Diverse Form Factors for Convenient Strong Authentication	3
Hardware OTP Tokens	4
Certificate-based Smart Cards	4
Certificate-Based USB Tokens	5
Smartphone and Software Tokens	6
Tokenless Authentication Solutions	6
Card Readers	7
About SafeNet Identity and Access Management Solutions	7

8 Page A4
Dec19
v43



2 Page A4
May 19
BBv1

thalescpl.com

THALES

CyberArk Privileged Access Security Solution and SafeNet Trusted Access



Today's organizations are constantly under the threat of social engineering and phishing attacks which result in compromised user identities and lead to costly security breaches. Thales and CyberArk work together to minimize the risks associated with hijacked credentials, by making it possible for organizations to enforce access management, SSO and multi-factor authentication at the point of privileged access by validating identities and enforcing access controls.

Key Benefits

- | | |
|---|--|
| <p>Adaptive Access Controls</p> <ul style="list-style-type: none"> Secure access to the CyberArk solution with minimal disruption to users | <p>Flexible Workflows</p> <ul style="list-style-type: none"> Enable administrators to have different authentication workflows based on the application of group membership |
| <p>Simplified Strong Authentication</p> <ul style="list-style-type: none"> Automated workflows provide flexible authentication options to secure users mitigating the reliance on passwords | <p>Protect Everything</p> <ul style="list-style-type: none"> Extend single-sign-on authentication to the CyberArk solution and other cloud applications, enabling centralized, secure access with a protected identity |

The Challenge

Securing users within an environment is becoming a crucial component to ensuring the security measures put in place offer complete protection. Applications and systems that are limited to a username and password, are no longer sufficient to protect your data and applications.

User identities are one of the primary attack vectors targeted by attackers' intent on breaching an organization and stealing sensitive resources. While any stolen user identity can have real consequences, privileged accounts are the primary target, as they provide unfettered access to an organization. To protect themselves organizations must implement a way to secure these sensitive accounts and track the systems that they are accessing.

The Solution

The best protection against the use of stolen or otherwise compromised credentials is strong adaptive access controls and multi-factor authentication that block attackers without disrupting legitimate users. Deploying multi-factor authentication and access controls aide organizations in thwarting a wide range of breach attempts by mitigating the potential of credential abuse – including pass-the-hash attacks, brute force attacks and more.

SafeNet Trusted Access integrates easily with CyberArk to provide an elegant solution that balances security and usability to protect privileged accounts from misuse at the identity perimeter.

Thales solutions are offered as a cloud service simplifying adoption and enabling organizations to automatically and rapidly deploy a strong layer of security without any additional infrastructure investment.

SafeNet Trusted Access and CyberArk Together

SafeNet Trusted Access enables administrators to create context-based, adaptive access policies that evaluate risk conditions and validates users by enforcing strong authentication where needed, ensuring the right people have access under the right conditions. A simplified user portal provides end users with a single access point to all configured applications, while granular access policies enhance security on sensitive apps, providing users with

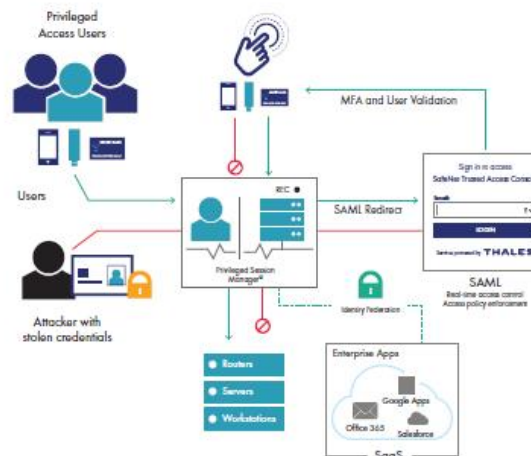
an SSO experience without compromising security or relying on static passwords. By setting up SafeNet Trusted Access as an IDP for CyberArk administrators can easily add a layer of strong authentication to CyberArk's privileged account security, protecting access to privileged accounts. This additional layer of security does not disrupt the user experience – in fact, it enhances it by providing authorized privileged users with single sign-on access to applications and resources across the enterprise.

About SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

About Cyberark

CyberArk is the global leader in privileged account security, a critical layer of IT security to protect data, infrastructure, and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reducing the risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 100, to protect against external attackers and malicious insiders. For more info, visit cyberark.com.



> thalescpl.com <



Amesbury – Thales eSecurity Inc., 2840 Lincoln Ave., San Jose, CA 95134 USA • Tel: +1 650 744 4916 • Fax: +1 954 880 4200 • E-mail: sales@thalescpl.com
Asia Pacific – Thales eSecurity & Security (HK) Ltd, Unit 4102-3, 41/F, Sunlight Tower, 240 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 2541 • E-mail: asia.sales@thales-cs.com
Europe, Middle East, Africa – Thales eSecurity, 10000 Boulevard de la Woluwe, 1200 Brussels, Belgium • Tel: +32 (0)2 220 0000 • Fax: +32 (0)2 220 0000 • E-mail: emea.sales@thales-cs.com

© Thales - May 2019 • BBv1



2 Page A4
Jun19
FRv5

thalescpl.com

THALES

How to become CJIS Compliant with SafeNet Trusted Access



Introduction

Cybercrime is recognized by the U.S. federal government as being a major threat to economic and national security. Indeed, numerous cyber attacks carried out in recent years have been aimed at government and state bodies. At the frontline of crime prevention, law enforcement agencies are vulnerable to network vulnerabilities, threats, and events which could undermine their professional abilities.

In order to ensure that law enforcement agents operate in a secure environment, the Criminal Justice Information Services Security Policy (CJIS-SP) defines requirements of timely availability of shared information and data confidentiality. The CJIS-SP must be adhered to by any organization that exchanges criminal records, including all local, state, and federal agencies that access and handle criminal justice information through its lifecycle—from creation through dissemination, whether at rest or in transit.

CJIS Authentication Requirements

To become compliant with CJIS-SP, law enforcement agencies need to implement advanced authentication (section 5.6.2.2) for cases where the risk of unauthorized access is high.

In order to successfully pass the triennial compliance and security audits by the FBI CJIS Division, CJIS-SP provides a list of advanced authentication methods that agencies can implement. Below are some guidelines that provide insight into how to select the advanced authentication method that is most appropriate to your agency.

Benefits

- **Fully automated**—Reducing the time and cost of provisioning, administration, and management of users and tokens.
- **Widest token choice**—Hardware, software, SMS, certificate/ PKI-based and passwordless authentication solutions accommodate multiple use cases and risk levels.
- **Low TCO**—Reducing the total cost of operation compared to traditional strong authentication environments.
- **Scalability**—A comprehensive solution prepared for growth and evolving needs based on the rapid changes in the threat landscape.

Choosing an Advanced Access Management and Authentication Solution

Consider a solution that offers a choice of 2FA (two factor authentication methods)

An access management and authentication solution that offers a range of multi factor authentication methods, and form factors allows organizations to address different levels of assurance. It also lets law enforcement officers choose their authentication method depending on their user preferences and security needs.

Consider a solution that will allow you to meet CJIS schedules in a timely manner

Service-based solutions that do not require extensive infrastructure investments allow agencies to shorten time to deployment considerably. Moreover, service-based solutions offer scalability and flexibility from a budget and user management perspective.

Consider a solution that meets TCO expectations.

There are several factors that lower the overall implementation and running costs of an access management and authentication solution:

- **Automated management workflows:** Access management and authentication solutions that offer automated provisioning and automated workflows typically require lower management
- **Self-service portals:** Offering comprehensive self-service functions to end users lowers help desk costs by allowing them to manage ongoing administrative tasks themselves.
- **Service-based delivery:** Service-based solutions eliminate infrastructure investments and maintenance costs, significantly lowering the total cost of operations and ownership.

About SafeNet Access Management and Authentication Solutions for CJIS compliance

SafeNet Trusted Access enables law enforcement agencies to meet the CJIS Security Policy for advanced authentication with a fully automated strong authentication solution that can be delivered as a cloud-based service or installed in a local data center.

SafeNet Trusted Access addresses numerous use cases, assurance levels, and threat vectors with unified, centrally managed policies—managed from one authentication back end delivered in the cloud or on-premises.

SafeNet Trusted Access offers fully automated provisioning, and user and token administration, significantly reducing management overhead and investments compared to traditional authentication solutions. SafeNet Authentication Solutions support the broadest range of authentication methods and form factors—all of which meet the CJIS requirement for advanced authentication.

Supported Authentication Methods

- OTP Push
- OTP Software
- OTP Hardware
- Pattern-based Authentication
- Out-of-band via email and SMS text messages
- Password
- Kerberos
- Google Authenticator
- PKI Credentials
- Passwordless Authentication
- Biometric
- 3rd Party

Easily extend MFA to cloud apps

SafeNet Trusted Access Management AND multi factor authentication in One

With SafeNet Trusted Access, businesses get the best of both worlds—a broad range of authentication methods combined with intuitive cloud-based access management and single sign on.

SafeNet Trusted Access easily lets you apply the multi-factor authentication methods deployed for VPNs to cloud and web-based applications. By federating your cloud apps via SAML or OIDC and applying the same authentication methods to both VPNs and cloud apps, organizations are able to achieve consistent access security across their IT ecosystem.

About Thales's SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

> thalescpl.com <

Americas - Thales Security Inc. 2840 Junction Ave, San Jose, CA 95134 USA • Tel+1 888 784 4976 or +1 954 888 6300 • Fax+1 954 888 6211 • E-mail: sales@thales.com
 Asia Pacific - Thales Security & Security (HK) Ltd, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel+852 2915 8633 • Fax+852 2915 8141 • E-mail: asia.sales@thales-security.com
 Europe, Middle East, Africa - Thales New York, Lang Cranden, Wyckoff, Basking Ridge NJ 07009 USA • Tel+44 (0)1844 201800 • Fax+44 (0)1844 208550 • E-mail: emea.sales@thales-security.com

© Thales - June 2019 • FR_V5



2 Page A4
Jun19
EHv3

thalescpi.com

THALES

Extending PKI smart cards to Cloud and Web Access Management



Extending your PKI smart cards and USB tokens to Cloud and Web Access Management

PKI-based authentication, cloud single sign-on and access management are no longer mutually exclusive. With SafeNet Trusted Access, organizations can use their current PKI smart cards to secure cloud and web-based applications.

PKI and Enterprise Digital Transformation

Cloud-based technologies and virtualized desktop infrastructure (VDI) offer enterprises cutting-edge productivity without the hassle of maintaining the underlying servers and workstations.

However, these technologies have not been compatible with PKI-based authentication, preventing organizations who use PKI-based smart cards from leveraging them for secure access in cloud and VDI environments.

As organizations transform their IT environments they are seeking ways to extend the security of PKI smartcards to virtual environments as well as cloud and web-based apps. They are looking for ways to offer employees Single Sign On and a consistent login experience across all apps; they are looking for ways to centrally manage their access policies, and ensure the appropriate access controls are applied for each online resource.

PKI Authentication in SafeNet Trusted Access




SafeNet Trusted Access validates the certificate and the PIN and grants user access.

SafeNet Trusted Access: Access Management AND PKI-based Authentication – In One

With SafeNet Trusted Access, businesses get the best of both worlds—high assurance PKI-based authentication combined with intuitive cloud-based access management. By incorporating PKI credentials into access management policies, organizations can apply SSO and PKI-based smart card authentication to apps residing in virtual, public and private cloud environments.

SafeNet Trusted Access – The Smart Way to Manage Cloud and Web Access

SafeNet Trusted Access is an access management service that centrally manages and secures access to web and cloud-based applications, simplifying the login experience for users. By applying flexible risk-based policies, cloud SSO, and universal authentication methods, organizations can scale cloud access controls while meeting business, risk management and compliance needs.

Applying PKI Security in Access Policies

SafeNet Trusted Access offers flexible access management through a simple to use policy engine that gives organizations real-time control over the ability to enforce policies at the group or application level. The policy engine supports a broad range of authentication methods, including PKI-based smart cards and OTP tokens, allowing organizations to leverage their current investments and use them to secure cloud and web-based services.

About SafeNet Access Management and Authentication Solutions


Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

Benefits of PKI-enhanced Access Management

By extending PKI smart cards to cloud and web based apps organizations can:

- Enforce high assurance security across cloud and web apps
- Effectively manage risk with business-driven policies
- Simplify access for users with cloud and web single sign-on (SSO)
- Demonstrate regulatory compliance while utilizing the cloud
- Elevate trust with a choice of PKI and OTP-based authenticators

© Thales - Jun 2019 - EH v3

> thalescpi.com < 

Americas – Thales eSecurity Inc, 2860 Junction Ave, San Jose, CA 95128 USA • Tel: +1 800 744 4574 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalescpi.com
Asia Pacific – Thales Transport & Security (HK) Co, Unit 4107-3, 41/F, Sunlight Tower, 249 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: sales.asia@thalescpi.com
Europe, Middle East, Africa – Thales New House, Long Canons, Aylesbury, Buckinghamshire HP18 9EG • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: amos.sales@thalescpi.com



2 Page A4
Jan-20
v5

thalesgroup.com

THALES

SafeNet FIDO2 Devices Arm your Enterprise with Strong & Secure Passwordless Authentication



As enterprises enter the 2020s, expand their digital transformation and move to the cloud, the majority of security breaches are related to identity theft. Many organizations have invested in strong authentication schemes, including PKI-based authentication.

These organizations now face the challenge of having to address new use cases, while maintaining the optimal balance between security and convenience.

How can organizations achieve a seamless and passwordless login experience from all devices? How can organizations address new use cases without having to rip and replace their authentication methods? Thales, the world leader in digital security, addresses these issues with two new SafeNet FIDO2 devices: the SafeNet IDPrime 3940 FIDO Smart Card and SafeNet eToken FIDO (USB token). These new solutions enable organizations to secure cloud adoption and bridge secure access across hybrid environments via an integrated access management and authentication offering.

Passwordless Authentication

Passwordless authentication replaces passwords with other methods of identity, improving the levels of assurance and convenience. This type of authentication has gained traction because of its considerable benefits in easing the login experience for users and surmounting the inherent vulnerabilities of text-based passwords. These advantages include less friction, a higher level of security that's offered for each app and the elimination of the legacy password.

Comfort for PKI Customers

One of the biggest benefits of the offering is organizations that rely on PKI authentication can now use a combined PKI-FIDO smart card to facilitate their cloud and digital transformation initiatives by providing their users with a single authentication device for securing access to legacy apps, network domains and cloud services.

FIDO2 and PKI Support, All in One Device

The SafeNet IDPrime 3940 FIDO Smart Card is designed for PKI-based applications and comes with a SafeNet eToken that offers perfect integration with active support for Microsoft environments, without any additional middleware.

The dual-interface smart card, allowing communication either via a contact interface or via a contactless ISO 14443 interface, is also compatible with some NFC readers.

SafeNet IDPrime 3940 FIDO Smart Card is CC EAL5+/PP Java Card certified for the Java platform and CC EAL5+/PP QSCD certified for the combination of Java platform and PKI applications. SafeNet IDPrime 3940 is qualified by the French ANSSI and is qualified according to the eIDAS regulations for both the eSignature and the eSeal applications. In addition, SafeNet IDPrime 3940 FIDO supports FIDO 2.0 standards.

USB Token with Touch Sense Options

The SafeNet eToken FIDO is a USB token, an ideal solution for enterprises looking to deploy passwordless authentication for employees. This authenticator is a compact, tamper-evident USB with presence detection, which creates a third factor of authentication: Something you have (physical token), something you know (PIN), something you do (touching the token).

Key Benefits

SafeNet FIDO2 Devices arm your enterprise with strong and secure passwordless authentication to any environment.

Key benefits include:

- Secure cloud adoption and bridge secure access across hybrid environments with a combined PKI/FIDO smart card.
- Secure & easy access on multiple operating systems.
- Passwordless access to cloud apps & external domains.
- Leverage your PKI authentication scheme—No rip & replace.
- Offer your users a single authenticator for all their needs.
- CC certified.
- Supports all devices and OS (without middleware deployment).
- Fully customizable.
- Ideal for digital signatures and email encryption.



thalescpl.com

THALES

Securing Identities Where and When Needed Large-Scale Identity and Certificate Management with SafeNet and Keyfactor



The Internet of Things (IoT) presents a huge business opportunity across almost every industry. But IoT also brings with it large scale, complex deployments that can cause security management challenges. As the scale of IoT deployments increases, the complexity of certificate lifecycle management increases. As the number of devices grows, companies need the ability to quickly and securely store and manage an expanding number of keys and certificates. As IoT devices are deployed and dispersed across the globe, an organization must be able to secure communications and to protect the data in motion to and from these devices.

The Solution – Securing & Managing Deployed IoT Security Systems

A strong, enterprise class, IoT security solution requires a combination of automated Public Key Infrastructure (PKI) certificate provisioning, firmware code signing, high-assurance key storage, and a powerful management system that simplifies certificate lifecycles while meeting data security and compliance requirements. Keyfactor and Thales bring together a solution of proven PKI and Key Storage solutions for both on-premises and in the cloud, combined with key lifecycle management systems to ease certificate deployments that handle the large scale and widely dispersed needs of IoT.

Thales has the depth of encryption and access management offerings to meet the needs of any deployment. With our Cloud 1st strategy we developed our HSM on Demand service, utilizing our deep industry experience and extends it to the cloud. And to protect applications and devices at the access point, Thales offers SafeNet Trusted Access, a cloud-based access management and authentication service. In addition to our industry-leading on-premises Luna HSM product line, Thales has partnered with Keyfactor to complete a flexible and powerful IoT offering.

- SafeNet Data Protection on Demand is a cloud based hardware security module (HSM) as a service that can be deployed within minutes and no need for specialized hardware or associated skills.
- SafeNet Luna HSMs store, protect and manage sensitive cryptographic keys on-premises in FIPS 140-2 Level 3, tamper-resistant hardware appliances, providing high-assurance key protection within an organization's own IT infrastructure
- Keyfactor Control enables device identity through a unique combination of certificate lifecycles management and automation at IoT scale and across all aspects of IoT ecosystem.
- SafeNet Trusted Access ensures secures identities and ensures secure access to devices and applications with a broad range of authentication methods.



Thales Use Cases for IoT:

1. Certificate Key issuance and management
2. Device Manufacturing Identity Provisioning PKI key issuance
3. Device and User Authentication during updates
4. Development and Update Code Signing
5. SSL/TLS Communication Private Key storage and management
6. Data at rest and data in motion security with advanced encryption entropy

Key Features

- Thales' SafeNet family of HSM solutions, either SafeNet Data Protection On Demand or Luna HSM, provide flexibility for cloud-based, hybrid/multi-cloud or on-premises root of trust protection and management of encryption keys.
- Keyfactor Control offers certificate lifecycle management that discovers, tracks and manages all credentials as well as providing code signing solutions for all classes of IoT devices, including embedded headless devices.
- SafeNet Trusted Access offers a broad range of authentication methods and adaptive access policies that evaluate risk conditions and validates users by enforcing the appropriate level of authentication where needed, ensuring the right people have access under the right conditions.

Solution Benefits

Many enterprises today need functionality of IoT with automated PKI capability and comprehensive certificate lifecycle management to meet the IoT security operation requirements of their deployments. The combination of Keyfactor Control, with Thales's SafeNet Luna HSM and the HSMoD service from SafeNet Data Protection On Demand provides:

Flexible HSM key protection solutions offer cloud, hybrid/multi-cloud and on-premises support that fit all deployments and meets the high-availability required for an IoT environment

- Device Identity Provisioning PKI key issuance during manufacturing establishes known device validation for its deployed lifecycle
- Device and user authentication assures identity before lifecycle events are performed
- Development Code Signing establishes strong, secure trust before device deployment
- Firmware Code Signing maintains trust during field software updates
- Automatic certificate discovery, inventory and issuance workflow reduces costs. Business continuity by avoiding certificate expirations that could cause expensive system outages
- SSL/TLS Private Key storage and management maintains secure communications during data exchanges with IoT devices. Offloading TLS/SSL operations increases system optimization
- Advanced encryption entropy ensure sensitive data at rest or in motion is secured

2 Page A4
Jul-19
ELCv3



2 Page A4
Jun-19
RMv13

thalescpl.com

THALES

SafeNet Trusted Access

Manage authentication deployments faster and more effectively



Why enterprises need cloud-based authentication services

More and more cloud-based services are becoming an integral part of the enterprise, as they lower costs and management overhead while increasing flexibility. Cloud-based authentication services, especially when part of a broader access management service, are no exception, and can help organizations achieve significant savings through automation. An effective access management and strong authentication service enables companies to pursue consistent access policies across the organization by creating a single pane of glass for access events, while securing a broad spectrum of resources, whether on-premises, cloud-based, or virtualized.

The solution: SafeNet Trusted Access

SafeNet Trusted Access delivers fully-automated, highly secure authentication-as-a-service with flexible authentication options tailored to the unique needs of your organization, while substantially reducing the total cost of operation. Strong authentication is made easy through the flexibility and scalability of automated workflows, vendor-agnostic token support, broad APIs and seamless out-of-the-box integrations with over 300

solutions from leading brands. With no infrastructure required, SafeNet Trusted Access enables a quick migration to a multi-tier and multi-tenant cloud environment, and protects everything, from cloud-based and on-premises applications, to networks, users, and devices.

Strong authentication made simple

- Utilize the multi-factor schemes already deployed in your organization and extend them to the cloud
- Deploy to thousands of users in 30 minutes!
- Apply access policies and achieve consistent security across your IT ecosystem
- Enable users an easy and simple log on experience with single sign on
- Reduce IT management overhead through automated user and token lifecycle administration
- Secure access to all IT resources with the broadest range of strong authentication methods

Key benefits

Low total cost of operation

SafeNet Trusted Access is based on a simple, low, per-user pricing model, with no hidden or additional costs.

Administration and management takes place in the cloud platform, reducing help desk expenses, and therefore lowering the management time by 90 percent, in most cases, through large-scale automation, token provisioning, and user self-enrollment.

Quick Cloud Migration

SafeNet Trusted Access has been designed to offer a smooth transition from an existing third-party RADIUS authentication server, focusing on speed and ease of deployment. Key to this capability is an organization's ability to maintain its current token investment while immediately benefiting from lower operational costs and automated processes. This reduces deployment time from weeks to hours, enabling organizations to easily move from an existing technology simply and quickly with a free migration agent.

Easy App Management

A continuously expanding library of integration templates enables the easiest connectivity to leading cloud apps, such as Salesforce, AWS and Office 365. Just use the integration templates already built-in and defined for the apps you use today, or use the general-purpose custom integration template.

Multi-factor and universal authentication methods



Features	Benefits
Fully Automated Workflows <ul style="list-style-type: none"> • Automated lifecycle administration synced with user stores • Escalated issue alerts delivered via SMS text messages or email • Self-service portal 	<ul style="list-style-type: none"> • Allows management by exception • Minimizes IT overhead required to provision, modify, and revoke access permissions • Self-service: <ul style="list-style-type: none"> • Allows users to report and resolve numerous issues by themselves • Reduces the cost of provisioning, administration, and management of users and tokens • Frees up IT resources to work on core tasks
Broad Use Case Coverage <ul style="list-style-type: none"> • Often access control to cloud applications, VPNs, VDI, portals, LANs • Hundreds of template-based integrations with leading services and apps • Supports third-party tokens and RADIUS servers 	<ul style="list-style-type: none"> • Allows quick and simple setup with ready-to-go configuration guides • Ensures smooth day-to-day performance • Single point of management lets you define policies once and enforce them throughout • Eliminates need for in-house development • Lets organizations maintain their current infrastructure and investments in tokens and IT solutions
Multi-Tier/ Multi-tenant Architecture <ul style="list-style-type: none"> • Scalability - Unlimited number of tiers and tenants makes it easy to accommodate complex organizational structures • Security - Complete segregation between subscriber accounts • Ideal for deployment and billing by Service Providers • Customization - Enables supporting the billing, security policies, branding and language of different customers from a single backend 	<ul style="list-style-type: none"> • Delegated management - Enables delegating administration and help desk support tasks to local or remote staff, making it easy to support different clients, regions, and groups • Centrally managed policies from a single backend • Reduces the cost of provisioning, administration, and management of users and tokens
Brandable and Customizable <ul style="list-style-type: none"> • Complete definition and control of your users' authentication journey • Brandable UI and portals • Multilingual support for user self-service, approval workflow, and enrollment 	<ul style="list-style-type: none"> • Minimal time required to customize and brand UI, portals, and workflows • Creates a unique user experience at no additional cost
Robust Reporting <ul style="list-style-type: none"> • Automated reporting • Ready-made templates for specific needs • Granular report fields allow report customization 	<ul style="list-style-type: none"> • Report templates minimize setup time • Automated report delivery • Minimize resources required to create and take action on reports

> thalescpl.com <

Americas - Thales Security Inc, 2840 Junction Ave, San Jose, CA 95134 USA • Tel: +1 888 744 4976 or +1 954 880 6200 • Fax: +1 954 880 6271 • E-mail: sales@thalessec.com
Asia Pacific - Thales Transport & Security (HK) Co, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 0633 • Fax: +852 2815 0161 • E-mail: asia.sales@thales-security.com
Europe, Middle East, Africa - Woodrow House, Long London, Mylesbury, Buckinghamshire HP18 9EJ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 206550 • E-mail: emea.sales@thales-security.com

© Thales - June 2019 - RM v13



2 Page A4
Aug-19
ELCv8

thalescpt.com



Thales and Palo Alto Networks Adding protection to the most sensitive area of your network – your users



The IT perimeter is changing and organizations need to be able to implement secure and seamless access to applications from any location for their users. By combining the solutions offered by Thales and Palo Alto Networks, organizations can implement access controls and deploy multi-factor authentication while balancing security and user experience.

The Challenge

Corporate infrastructures are changing and the traditional IT perimeter is becoming blurred as more organizations diversify and are faced with maintaining security in hybrid deployments which consist of a mix of legacy, custom, and cloud applications.

Some legacy or custom applications may not always support the use of anything other than a password. This becomes problematic as studies have highlighted that 81% of data breaches are due to stolen or weak passwords¹.

Securing users within an environment is becoming a crucial component to ensuring the security measures put in place offer complete protection. Deploying multi-factor authentication and access controls aide organizations in thwarting a wide range of breach attempts by mitigating the potential of credential abuse – including pass-the-hash attacks, brute force attacks and more.

¹ Verizon 2017 Data Breach Investigation Report



By deploying Palo Alto Networks Next Generation Firewall with Thales's Authentication and Access Management solutions you can streamline deployment of strong authentication and increase the protection of your infrastructure efficiently without needing to replace any existing components.

Key Benefits

- Versatile integration methods to support hybrid deployments
- Automated multi-factor token lifecycle management
- Enforce strong authentication based on risk evaluation of network, device OS and location
- Centrally manage access policies for applications
- Reduced IT helpdesk and infrastructure costs
- Prevents unauthorized access
- Enables compliance with security regulations
- Supports OOB/Push authentication
- Balances Security with Usability
- Unlimited Software Tokens
- Multiple Authentication methods per user supported

Thales's Authentication and Access Management Solutions

Thales's SafeNet Trusted Access combines easy to deploy access management and strong authentication allowing organizations to balance security with the end user experience. SafeNet Trusted Access enables administrators to create access policies that evaluate risk conditions and validates users by enforcing strong authentication where needed, ensuring the right people have access under the right conditions.

Thales solutions are offered as a cloud service simplifying adoption and enabling organizations to automatically and rapidly deploy a strong layer of security without any additional infrastructure investment.

Thales and Palo Alto Networks

While Palo Alto Networks Next-Generation Firewall inspects traffic, enforces network security policies, and delivers threat prevention, Thales's SafeNet Trusted Access solution adds additional risk evaluations and enforces the need for strong authentication where needed. With the strong, multi-factor authentication offered by Thales, weak passwords are replaced by an additional security layer that validates users, and logs their access attempts for audit purposes. By combining Palo Alto Networks Next-Generation Firewall with Thales's strong authentication and access management solutions businesses can meet strict compliance requirements with an elegant solution that ensures the utmost in network protection.

Strong Authentication

SafeNet Trusted Access platform supports a wide range of two-factor authentication options, including traditional AD password, hardware tokens, software tokens, web-based tokens and certificate based authenticators. This allows users to authenticate from anywhere at any time. With access policies, organizations can define what type of authentication is needed, and offers the capability to combine authentication methods. SafeNet's MobilePass* supports out-of-band push authentication on mobile devices which provides a streamlined user experience while enforcing a strong authentication method. By leveraging the existing user repository organizations can set up automation policies that will provide users with an authentication method without IT involvement. The simple and user friendly self-service options empower users to adopt the use of multi-factor authentication in a frictionless way which increases user deployment without overburdening the IT helpdesk.

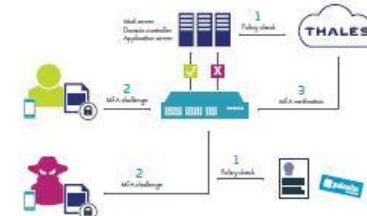
Powerful Access Controls and Centralized Management

Access policies can be set up in SafeNet Trusted Access based on application or group membership, centralizing the management of security policies against the entire environment. Integration options enable organizations to protect their GlobalProtect and extend the

> thalescpt.com <

Americas – Alhambra Plaza II, 3442 Capital of Texas Highway North, Suite 300, Austin, TX 78759 USA • Tel: +1 888 243 5772 or +1 512 257 3900 • Fax: +1 954 888 6211 • E-mail: sales@thales.com
Asia Pacific – Thales Transport & Security (HK) Ltd, Unit 4103-3, 41/A Sunlight Tower, 245 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 9633 • Fax: +852 2815 9840 • E-mail: asia.sales@thales-security.com
Europe, Middle East, Africa – Alhambra New York, Long London, Highbury, London Greater London SE18 6PS • Tel: +44 (0)1844 208530 • Fax: +44 (0)1844 208530 • E-mail: emea.sales@thales-security.com

© Thales August 2018 • ELCv8



enforcement of multi-factor authentication to all the applications in their environment. The flexible policy engine permits administrators to set policies which evaluate risk conditions and implements stronger controls for users who are accessing resources from older operating systems and mobile devices, or augment the firewall policies set in the Palo Alto Networks devices to deny access from certain geographic locations. Add further protection with SafeNet Trusted Access to other sensitive applications by setting policies which require multiple authentication methods. All of this is managed through a centralized console which provides real-time analytics and empowers administrators to quickly and easily adjust policies based on business and compliance requirements.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

About Palo Alto Networks

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and endpoints. Find out more at <https://www.paloaltonetworks.com>



thalespl.com

THALES

Implementing Authentication and Access Controls for Office 365



Thales's solution SafeNet Trusted Access makes it easy to implement Access Controls and Strong Authentication with Microsoft Office 365, offering robust application protection that is convenient for end-users.

Office 365: The Challenges

Deployment of Office 365 creates a new reality for organizations in which employees, whether in the office, at home, or on the road, can access enterprise systems remotely. By default the only protection afforded these online services are inherently weak, static passwords. With nearly 60% of organizations, sensitive data being stored in the cloud and over 71% of deployments experiencing at least one compromised account each month¹; implementing access controls that evaluate risk profiles and implement strong authentication is crucial.

SafeNet Trusted Access: The Solution

SafeNet Trusted Access by Thales is an intelligent access management service that allows customers to enforce the perfect balance between user convenience and secure access to all apps across their organization.

SafeNet Trusted Access offers flexible access management through a simple to use policy engine that gives customers real-time control over the ability to enforce policies at the individual user, group or application level. The policy engine supports a broad range of

Key Benefits

- | | |
|--|--|
| <p>Reduced Total Cost of Ownership (TCO)</p> <ul style="list-style-type: none"> Leverages existing infrastructure and reduces management overheads through automation. Implements strong multifactor authentication which reduces password fatigue and lowers helpdesk costs. | <p>Increased Productivity</p> <ul style="list-style-type: none"> Offers users a convenient, hassle-free single sign-on (SSO) experience Adaptive authentication policies that evaluate risk balance security and convenience. |
| <p>Simplified Administration</p> <ul style="list-style-type: none"> Eliminates complex integration, and ensures easy management with a cloud service that can be set up and running in a couple of hours | <p>Protect Everything</p> <ul style="list-style-type: none"> Secures access to Office 365 and all other cloud/web-based apps with a single access management service |

¹ Source: Office 365 Adoption Rate, Stats, and Usage

authentication methods, including ones already deployed, allowing organizations to leverage their current investments and use them to secure cloud and web-based services.

By combining SSO, risk-based policies and universal authentication methods, SafeNet Trusted Access gives organizations the power and flexibility to secure access to all apps, simplify the login experience, and effectively manage risk.

Securing Access to Office 365: How it Works

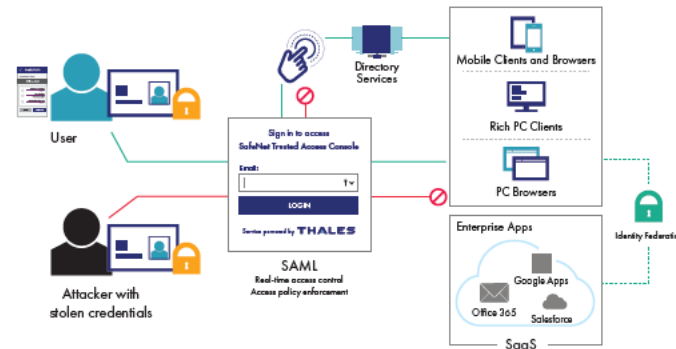
SafeNet Trusted Access leverages existing infrastructure investments and simplifies the process of implementing access controls to validate user identities. Through a simple, template-based, SAML 2.0 integration, SafeNet Trusted Access acts as the trusted identity provider for Office 365 and other third-party cloud and web-based apps, providing IT administrators with the ability to easily deploy an access management solution across their entire environment. SafeNet Trusted Access is a cloud-based service, ensuring a speedy deployment and easy maintenance - with no additional administrative overhead or changes to existing infrastructures.

About Thales's SafeNet Identity and Access Management Solutions

Thales's industry-leading Identity and Access Management solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively manage risk, maintain regulatory compliance, gain visibility into all access events and simplify the login experience for their users.

Key Features

- An intuitive administrative console lets administrators configure and adjust policies for applications and groups of users quickly and easily.
- Optimizing security with convenience, administrators can choose to enforce single factor or multi-factor authentication through defined access policies and are able to layer authentication options to increase or relax requirements where needed. Users can access all their apps and initiate an SSO session from a customized app portal.
- The solution supports numerous authentication methods giving organizations a wide variety of options to mitigate risk. Universal authentication options supported include out-of-band (OOB) authenticators (PUSH or SMS), pattern-based authenticator (PIP), hardware and software-based one-time password (OTP) form factors, third-party authenticators, PKI certificate-based authentication, and Kerberos.



> thalespl.com <

North America - Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • Email: sales@thalessec.com
Asia Pacific - Thales Transport & Security (UK) Ltd, Unit 4101-3, 41/F, Sunlight Tower, 240 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2915 9638 • Fax: +852 2915 9441 • Email: asia.sales@thales-ecsecurity.com
Europe, Middle East, Africa - Thales eSecurity Ltd, 10000, Longwalk Road, Longwalk, Middlesex, UK • Tel: +44 (0)1844 208550 • Fax: +44 (0)1844 208550 • Email: emea.sales@thales-ecsecurity.com

© Thales - May 2019 - BBv1



2 Page A4
Oct-19
RM7

thalescp.com

THALES

SafeNet IDPrime PIV



Personal Identity Verification-interoperable ID credentials for federal agencies, government contractors, state and local governments and private sector organizations

SafeNet IDPrime PIV (Personal Identity Verification) card is a FIPS 201 standards-based card for U.S. government agencies, state and local government organizations to issue user credentials that the Federal Government can trust. The same card can be used for either a CIV or PIV-I based deployment depending on company policies and requirements. This smart card provides premium privacy protection through mandatory and optional features of the SP800-73-4 standard. Customers can benefit from enhanced performance and built-in biometric capabilities (On Card Comparison), preparing them for enhanced user authentication.

Uses of PIV

- Based on strong multi-factor PKI authentication, SafeNet IDPrime PIV cards provide proof of cardholder identity that meets U.S. Federal Government standards
- Digitally authenticates users' identity for main information systems
- Identifies users for a variety of physical access systems
- Digitally signs and encrypts documents, email and files
- Works with Federal Government PIV-based IT infrastructures, and new and legacy physical access control systems
- Biometric fingerprint and iris delivers highest level of identity assurance

Features

- Virtual Contact Interface (VCI) and Pairing code to enhance privacy through contactless interface, for physical access use cases
- PIV Secure Messaging to provide confidentiality and integrity protection to PIV card application
- Biometric Authentication (On Card Comparison), compliant to SP800-76-2, for enhanced user authentication
- Fast contactless authentication with an optimized Power-On-Self-Test mechanism as per the latest FIPS 140-2 specifications (CMVP IG 9.11)

PIV Technology and Standards

PIV card technology features a dual interface microprocessor chip for use with contact and contactless smart card readers, making it interoperable and easily adaptable for a wide range of use cases, including physical access authentication. SafeNet IDPrime PIV cards are certified FIPS 140-2, security level 2, FIPS 201-2 and listed on the GSA APL.

PIV and the U.S. Federal Government

Most U.S. federal government employees and subcontractors have a PIV card. Driven by the issuance of Homeland Security Presidential Directive 12 (HSPD-12) in 2004, the U.S. federal government has invested significant effort and resources in implementing robust, interoperable credentialing processes and technologies. The resulting standard, FIPS 201, Personal Identity Verification (PIV) for federal employees and contractors, provides a framework of the policies, processes, and technology required to establish a strong, comprehensive identity credentialing program.

Government Contractors and Critical Infrastructure Organizations

Implementing PIV-I identity credentialing and security systems helps enterprises, including those involved with the nation's critical infrastructure, to significantly upgrade the security of their information systems and networks. In addition, the fact that PIV-I credentials are trusted and interoperable with the federal government makes it much more efficient and secure for contractors to exchange information securely with their government clients. It also creates opportunities to improve business processes, such as digitally signing and encrypting contracts or specifications.

State and Local Government

State and local governments can leverage the federal PIV program by using PIV-I as the basis for their identity credentialing and information system security. Many point to the PIV standard as a way to achieve a more holistic approach to issuing identity credentials and improving their own business processes and information systems security. More than 16 states are currently planning or implementing some form of PIV-I or CIV (Commercial Identity Verification) strategy. PIV-I credentials are being used in regional and national interoperability exercises sponsored by the Federal Emergency Management Agency (FEMA) for First Responder Access Cards (FRAC). These credentials, typically issued by state and local governments, identify emergency responders for secure access to remote networks to pilot operations and access to Federal systems.

About SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance. To learn more, please visit our website at safenet.gemalto.com/access-management/

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Technical Specifications

Memory	SafeNet IDPrime PIV card is based on a Java Card platform (JCCore 310) with 146 KB EEPROM memory with PIV v3.0 applet loaded.
Certifications	FIPS 140-2 Security level 2, FIPS 201-2, and listed on GSA APL (with the certificate #1510) <ul style="list-style-type: none"> Roles, Services, and Authentication: Level 3 Physical Security: Level 3 EMI/EMC: Level 3 Design Assurance: level 3 SCPO3, SCPO2, SCPO1 supported with scripting according to GP 2.2.1 Amendment Amendment D ECC (256, 384). Asymmetric algorithms supported and FIPS certified
Cryptographic algorithms	Hash - SHA-224, SHA-256, SHA-384, SHA-512, SHA-1 Symmetric - AES (128-, 192-, 256-bit) Asymmetric - ECC (P-224, P-256, P-384, P-521 bits), RSA (up to RSA 4096 bits) using an on-card security controller with key pair generation and Deterministic Random Bit Generator (DRBG)
ISO specification compliance	<ul style="list-style-type: none"> ISO 7816 contact interface (T=0; T=1) ISO 14443 contactless interface compatible with NFC (F=C1) IJ high coercivity magnetic stripe (optional)
Other features	<ul style="list-style-type: none"> Global PIN and local PIN Dynamic Discovery Object management during post issuance Dynamic Contactless interface de-activation mechanism Fingerprint and its biometric containers Up to 20 Key archiving containers

> thalescp.com <



Americas - Ardmore Plaza II, 9402 Capital of Texas Highway North, Suite 300, Austin, TX 78759 USA • Tel: +1 800 343 6773 or +1 512 257 2900 • Fax: +1 954 888 6271 • E-mail: sales@thales.com
Asia Pacific - 10th Floor, 1500 Market Street, Suite 1000, San Francisco, CA 94102 USA • Tel: +852 2915 8623 • Fax: +852 2915 8141 • E-mail: asia.sales@thales.com
Europe, Middle East, Africa - Watford New House, Long Green, Watlington, Oxfordshire OX11 9SD • Tel: +44 (0)1844 291800 • Fax: +44 (0)1844 291550 • E-mail: emea.sales@thales.com

RM7 - October 2019 - Thales



thalescpl.com

THALES

Access Management Primer What is Cloud Access Management and Who Needs It?



Who's Afraid of Cloud Apps?

Cloud applications are excellent at providing organizations the best technology at a quick time to value, zero maintenance overhead and infinite scalability. The immediate fulfillment and instant productivity provided by cloud apps comes, however, with a price tag. IT departments lose visibility into who is accessing what application, when—and what authentication method is being used. And this is true for IT-vetted applications as it is with shadow IT apps procured and implemented by individual departments. Compliance risk increases as apps are managed from multiple disparate consoles, while help desk tickets owing to password resets abound. And the most important person in the process—the end user—suffers from password fatigue, frustration and downtime as they fret to keep their copious identities in order.

Cloud Access Management 101

To address these cloud adoption hurdles, cloud access management solutions have emerged to streamline cloud access provisioning, eliminate password hassles for IT and users, provide a single pane view of access events across your cloud estate and ensure that the right access controls are applied at the right time to the right user.

Put simply, **cloud access management ensures that the right people have access to the right applications at the right level of trust.**

Cloud access management solves the challenges faced by enterprises in their quest for broader cloud adoption.

Access Management Benefits

Implementing cloud access management solutions increases enterprise access security, removes the ambiguity associated with cloud security and compliance risk—and no less important—ensures the most frictionless user experience.

Organizations that incorporate cloud access management into their cloud adoption strategy enjoy benefits across the business.

Enhanced user convenience

Access management solutions offer cloud single sign on, which lets your users log in just once in order to gain access to all their cloud applications, using the familiar enterprise identity they already use today. This means that users no longer need to maintain disparate username and password sets for each cloud application, but rather need only maintain one!

Optimized cloud security

By enforcing scenario-based access controls using finegrained policies, organizations optimize security and reduce the risk of a breach. By factoring in variables such as privileged user accounts, the sensitivity of high-value applications, and contextual parameters, administrators can tailor cloud access policies to the scenario at hand. Furthermore, the access journey is made painless for users as policies are defined to require stronger forms of authentication only when needed.

Ease of Management

Access management provides administrators with a single point of management, a single pane of glass, from which to define access policies once and enforce them throughout. By replacing disparate cloud admin consoles with just one, IT departments can scale cloud adoption while maintaining security and visibility across their cloud estate.

Plus, by having to maintain just one identity per user for all their cloud applications, IT departments eliminate help desk tickets associated with password resets, which account for 20% of help desk tickets annually.

Built with the cloud in mind, many access management solutions make it easy to integrate new cloud applications, letting you cast light on shadow IT and on-board new apps as your business needs evolve.

Visibility

Access management solutions enable IT to answer the questions "Who has access to what?" "Who accessed what and when?" and "How was their identity verified?" By gaining a central view of access events, coupled with authentication methods, organizations gain visibility into cloud access events for easy compliance audits and tracking.

Visibility into which applications are being accessed also saves businesses money as it enables identifying which app licenses are underutilized.

Cloud access management offers benefits across the business:

- Enhanced user convenience
- Optimized cloud security
- Ease of management
- Visibility

Access Management—The Smart Way to Manage Cloud Access

Cloud access management solutions are the smart way to manage cloud applications in your organizations. By providing single sign on to users and enforcing granular access policies that enforce the right level of authentication at the right time, you can provide your user community with the most frictionless authentication journey possible. Replacing the binary yes/no authentication decisions of yesterday, access management addresses the multifaceted security management and compliance challenges of cloud adoption in the enterprise.

About SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud based applications. Utilizing policybased SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

> thalescpl.com <

Americas – Thales eSecurity Inc, 2840 Junction Ave, San Jose, CA 95134 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalessec.com
Asia Pacific – Thales Intrust & Security (HK) Co, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia_sales@thales-security.com
Europe, Middle East, Africa – Thales Group, Longwalk Road, Basingstoke, Hampshire RG24 0BA UK • Tel: +44 (0)1256 343000 • Fax: +44 (0)1256 343001 • E-mail: emea_sales@thales-security.com

© Thales - May 2019 • BBv1

2 Page A4
May-19
BBv1



thalescpl.com

THALES

SafeNet Trusted Access Cloud-based Access Management as a Service



Cloud Adoption in the Enterprise

Cloud based applications play a vital role in fulfilling productivity, operational and infrastructure needs in the enterprise. However, the burden of managing users' multiple cloud identities grows as more cloud apps are used. Each new service added to an organizations' cloud estate, makes unified visibility into cloud access events harder to achieve, and increases compliance risk. Users struggle to maintain countless usernames and passwords, while help desk tickets requiring password resets abound. And with cloud applications protected, by default, only with weak static passwords, the risk of a data breach rises.

Cloud Access

SafeNet Trusted Access addresses these challenges:

An access management service that centrally manages and secures access to web and cloud-based applications, SafeNet Trusted Access simplifies the login experience for users. By applying flexible risk-based policies, cloud SSO, and universal authentication methods, organizations can scale cloud access controls while meeting business, risk management and compliance needs.

Organizations can easily secure cloud apps and meet risk management needs by building on their current security frameworks and leveraging existing authentication schemes for cloud access.

How It Works

Each time a user logs in to a cloud application, SafeNet Trusted Access:

- Validates the user's identity
- Assesses which access policy should be applied
- Applies the appropriate level of authentication with Smart Single Sign-On.

SafeNet Trusted Access Benefits

SafeNet Trusted Access prevents data breaches and helps organizations comply with regulations, allowing them to migrate to the cloud simply and securely.

Prevent breaches

- Apply different MFA methods and control accesses for each app while eliminating passwords

Enable cloud transformation securely

- Extend existing access controls to cloud apps and apply consistent access policies to all cloud resources

Simplify compliance

- Prove compliance with a real-time audit trail of who is accessing which app and how

SafeNet Trusted Access Core Capabilities

SafeNet Trusted Access offers enterprises five core capabilities.

- 1. Smart Single Sign-On.** Smart Single Sign-On lets users log in to all their cloud applications with a single identity, eliminating password fatigue, frustration, password resets and downtime. SafeNet Trusted Access processes a user's login requests and ensures that SSO is applied intelligently, based on previous authentications in the same SSO session and the specific policy requirements applicable to each access attempt. In this way, users may authenticate just once in order to access all their cloud applications, or provide additional authentication as configured in the policy.
- 2. Scenario-based Access Policies.** SafeNet Trusted Access offers flexible access management through a simple to use policy engine that gives customers real-time control over the ability to enforce policies at the individual user, group or application level. The policy engine supports a broad range of authentication methods, including ones already deployed, allowing organizations to leverage their current investments and use them to secure cloud and web-based services.
- 3. Data-driven Insights.** Data-driven insights into access events enable organizations to fine-tune their access policies, and ensure that they are neither too lax nor too stringent. Statistics and logs on access activity per app and per policy, along with the reason for failed or denied access attempts, facilitate audits and support inquiries, and allow identifying underutilized cloud app licenses.
- 4. Universal Authentication.** SafeNet Trusted Access supports numerous authentication methods and allows you to leverage authentication schemes already deployed in your organization. The broadest range of authentication methods and form factors supported combined with context-based authentication enhances user convenience and allows you to manage risk by elevating trust only when needed.
- 5. Easy App Management.** A continuously expanding library of integration templates enables the easiest connectivity to leading cloud apps, such as Salesforce, AWS and Office 365. Just use the integration templates already built-in and defined for the apps you use today, or use the general-purpose custom integration template.

Supported Authentication Methods

- OTP Push
- OTP App
- OTP Hardware
- Pattern-based authentication
- Out-of-band via email and SMS text messages
- Password
- Kerberos
- PKI credentials
- Google Authenticator
- Passwordless authentication
- Biometric
- Voice
- 3rd party

About SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

To learn more about access management from Thales, visit <https://safenet.gemalto.com/access-management/> or join a live demo webinar at <https://www.brighttalk.com/webcasts/2037/334449>

Access Management for Leading Applications

SafeNet Trusted Access supports hundreds of applications, including the following:



> thalescpl.com <

Americas – Thales Security Inc, 2340 Junction Ave, San Jose, CA 95134 USA • Tel: +1 888 744 4576 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalessec.com
Asia Pacific – Thales Transport & Security (HK) Ltd, Unit 4101-2, 41/F, Sunlight Tower, 240 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8623 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-security.com
Europe, Middle East, Africa – Thales New Horizons, Long Courcier, Meybeck, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: www.sales@thales-security.com

© Thales - May 2019 • DB-14

2 Page A4
Jan-20
BB V15

Adapted for
Delegate Bag

STA CIAB
EDM1



thalesgroup.com

THALES

Passwordless Authentication: How Giving Up Your Password Might Make You More Secure



White Paper

Why Passwords Are Bad

Passwords are one of the oldest security tools in the world of software and the internet. But in today's environment, passwords cannot provide enough protection for businesses for several reasons.

Password Fatigue Leads to Bad Hygiene

Policy-driven password strengths and rotation leads to password fatigue, thereby contributing to poor password management. Verizon's Data Breach Investigation Report¹ indicates that **over 70 percent of employees reuse passwords** for work and personal accounts. A malicious actor could therefore abuse an employee's credentials to access other applications and sensitive customer information.



81%
of breaches involve
use of weak or
stolen credentials



~40
Average person
has roughly 40
online accounts



4 out of 5
People reuse same
passwords across
different accounts



"123456"
"password"
still among most
popular password
choices in 2018

People also tend to pick easy-to-hack passwords because of the trouble they have with remembering passwords. An analysis of over five million leaked passwords showed that 10 percent of people used one of the 25 worst passwords². Seven percent of enterprise users had extremely weak passwords.

Passwords Hurt User Experience

Research by Carnegie Mellon University indicates that a properly written password policy can provide an organization with increased security. However, there is less accord over what should be in this policy to make it effective. To illustrate this fact, users commonly react to a policy rule that requires them to include numbers by picking the same number or by using the number in the same location in their passwords³.



Some password policies may make passwords difficult to remember or type. In response, users can undermine the security of their passwords by writing them down, reusing them across different accounts or sharing them with friends. They also frequently forget them, creating more work for the helpdesk.

Passwords Can Hinder User Security

Ironically, passwords can be a detriment to security by serving as an attack vector. According to Verizon's Data Breach Investigations Report in 2018, **81% of hacking-related breaches** were a result of weak, stolen, or reused passwords⁴. Threats like man in the middle attacks and man-in-the-browser attacks take advantage of users by mimicking a login screen and encouraging the user to enter their passwords. It's even more unsafe in the cloud. Login pages hosted in the cloud are completely exposed, thus enabling a bad actor to carry out phishing or brute force attacks against publicly known login pages like outlook.com.

¹ <https://enterprise.verizon.com/resources/reports/dbi/>
² https://www.ble.com/en_us/article/popular/100-many-people-are-still-using-password-as-a-password
³ <https://openstax.org/r/why-passwords-are-bad>
⁴ https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf



thinkupLabs

THALES

Assessing the True Cost of Strong Authentication

The Total Cost of Operation of On-premise vs. Cloud-based Authentication



White Paper

Contents

- 03 The True Costs of Authentication – Hard Costs vs. Soft Costs
 - 04 Soft Costs
 - 06 Hard Costs
- 07 Putting Costs into a TCO Perspective
- 07 The Affordability of Cloud-based Authentication
- 08 Conclusion
- 08 Key Benefits
- 08 About Thales

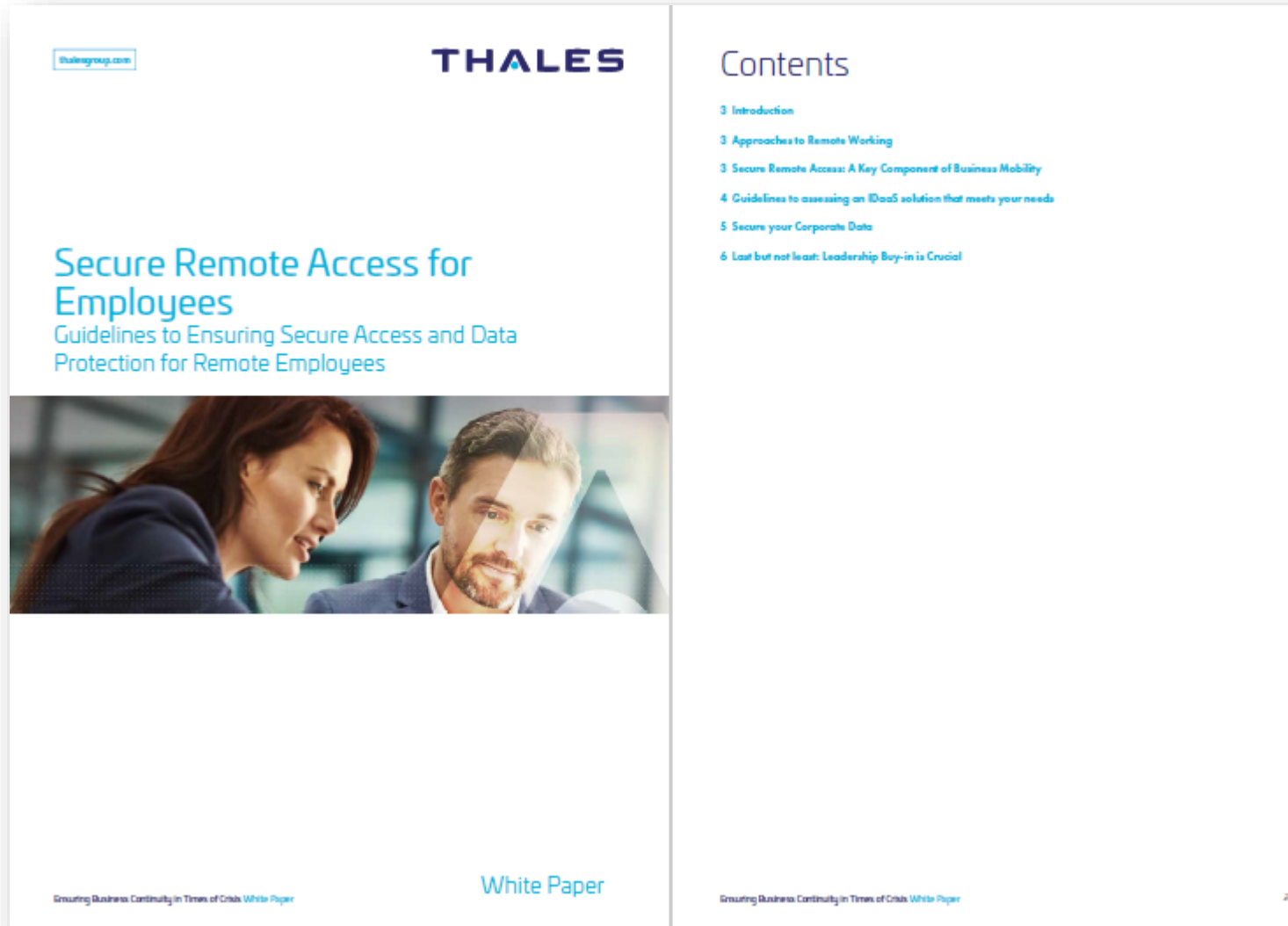
Assessing the True Cost of Strong Authentication - White Paper

2

9 Page A4
Jun-19
ELCv2



7 Page A4
Mar20
DBV3





13 Page A4
Mar20
DBV3

The image shows a preview of a white paper document. The left side is the cover page, and the right side is the contents page.

Cover Page:

- Top left: thalsgroup.com
- Top right: **THALES**
- Center: **Protecting O365 and Microsoft Environments with Thales' SafeNet Trusted Access**
- Image: A photograph of a woman and a man in business attire looking at a laptop screen.
- Bottom right: **White Paper**

Contents Page:

- Contents**
- 3 Introduction
- 3 Access Challenges in Cloud Environments
- 4 Mitigating Cloud-based Access Management Challenges
- 5 Factors to Consider when Assessing an IDaaS Solution
- 6 Protecting Microsoft Cloud-Based Environments with SafeNet Trusted Access
- 12 Conclusion

Abstract

Organizations are on a cloud migration journey. Many organizations that have implemented various on-premises Microsoft solutions, such as Office suite and AD FS, are now migrating some of these Microsoft solutions – primarily Office 365 – into the cloud. Security of these cloud-based services is of the utmost importance. In this white paper, we'll discuss how SafeNet Trusted Access, Thales' cloud-based access management and authentication service, can help your organization protect your Microsoft cloud-based services and scale securely in the cloud.

Protecting O365 and Microsoft Environments with Thales' SafeNet Trusted Access *White Paper* 2




13 Page A4
Sep19
FR v7

thalescpt.com

THALES

Before you Choose AD FS: 5 Considerations in Assessing an SSO Solution



Information and specifications described herein are true at the time of publication and are subject to change without notice.

White Paper

Contents

- 03 Executive Summary
- 03 Introduction
- 04 Consideration #1: Costs
- 06 Consideration #2: Automation
- 07 Consideration #3: Authentication
- 08 Consideration #4: Availability
- 09 Consideration #5: Security
- 10 Conclusion
- 11 About SafeNet Trusted Access: The Smart Way to Manage Cloud Access
- 11 About Thales's SafeNet Access Management and Authentication Solutions
- 12 Appendix
- 12 References

Figures

- 04 Table 1: AD FS Hard and Soft Costs
- 06 Table 2: AD FS Automation
- 07 Table 3: AD FS Authentication Methods
- 08 Table 4: AD FS Uptime and Service Levels
- 09 Table 5: AD FS Security Comparison
- 12 Table 6: Enterprise Self-Assessment Tool: Microsoft AD FS vs. Thales SafeNet Trusted Access

Before you Choose AD FS: 5 Considerations in Assessing an SSO Solution White Paper 2



cpl.thalesgroup.com

THALES

A Comprehensive Guide to Authentication Technologies and Methods



White Paper

Contents

- 03 Introduction – On Digital Identities and Authentication
- 03 Methods of Authentication
- 07 Classes of Attacks on Authentication Mechanisms
- 09 Analysis of Authentication Mechanisms
- 13 Key Considerations for Selecting an Authentication Method
- 13 Conclusion
- 15 About Thales

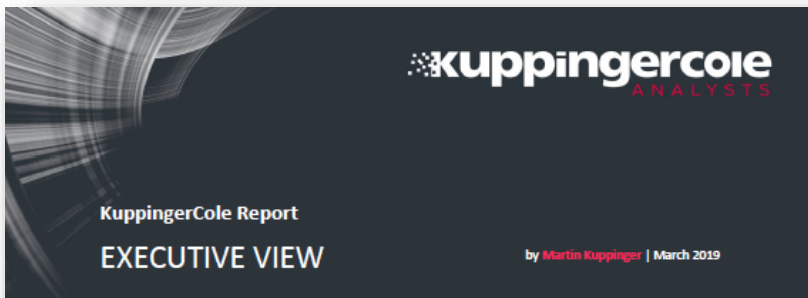
A Comprehensive Guide to Authentication Technologies and Methods White Paper

2

13 Page A4
Mar20
IELC, v2



7 Page A4
May19



Vormetric Application Crypto Suite

Encryption, tokenization, and data masking are essential capabilities needed in today's highly regulated environments. Protecting sensitive information requires these capabilities, beyond just network and file-level encryption. Vormetric Application Crypto Suite from Thales eSecurity provides an integrated, easy-to-use set of services covering the needs for such environments.



by Martin Kuppinger
mik@kuppingercole.com
March 2019

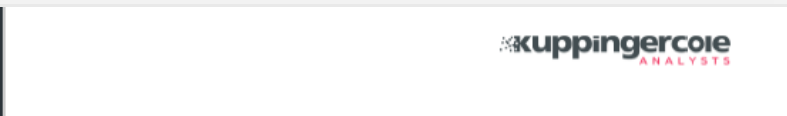
Content

1 Introduction	2
2 Product Description	3
3 Strengths and Challenges	5
4 Copyright	6

Related Research

- Leadership Compass: Privilege Management - 72330
- Architecture Blueprint: Hybrid Cloud Security – 72552
- Leadership Brief: Six Key Actions to Prepare for GDPR – 70340
- Leadership Compass: Database Security – 70970

KuppingerCole Executive View
Vormetric Application Crypto Suite
Report No.: 79069



1 Introduction

With an ever-growing number of cyberattacks and ever-increasing regulations, businesses are under constant pressure to properly protect their sensitive data sets. Such protection is needed at various levels and includes several elements, from endpoint protection and network firewalls to IAM (Identity and Access Management), CASBs (Cloud Access Security Brokers), and others.

Last, but not least, amongst these technologies is encryption. Encryption can be implemented (and regularly is implemented) at various levels. Network encryption, e.g. based on the SSL/TLS standard, is ubiquitous when using the Internet. Disk encryption is widely supported on both clients and servers. File systems can be encrypted as well. Finally, data encryption enables the encryption of specific sets of data for specific applications or at the database level.

Data encryption provides, for example, enhanced protection of sensitive data such as credit card numbers, patient data in healthcare, passports or other types of PII (Personally Identifiable Information). Thus, it also helps in compliance with regulations that require specific, in-depth protection of sensitive data such as

- PCI DSS, which requires specific protection of credit card information;
- HIPAA/HITECH, which requires specific protection of healthcare information.
- GDPR, which raises the bar for protecting PII

In addition, there are many other use cases, well beyond PII protection. Many businesses also want and need to specifically protect financial information or intellectual property. Depending on where that information resides, different approaches to protecting, and specifically encrypting, that information are required.

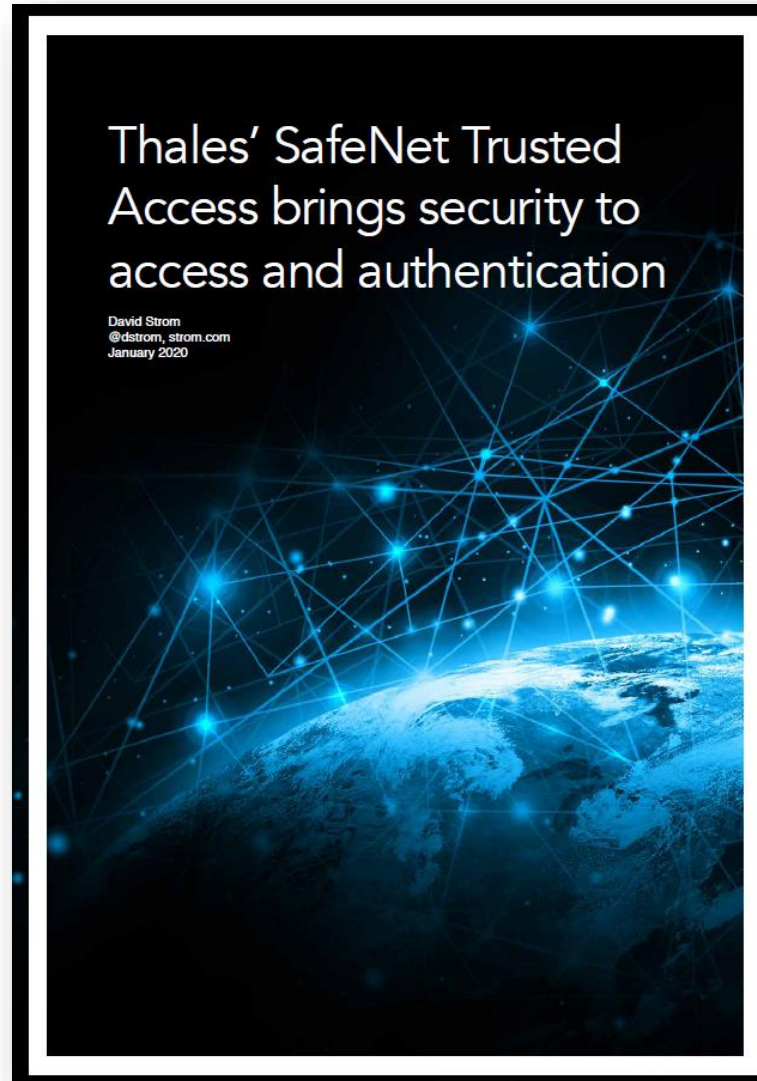
Common approaches for encryption focus either on data at rest, i.e. held on some sort of storage, or data in motion, i.e. during the transfer of data. For the latter, we can distinguish between end-to-end solutions that encrypt information all the way between endpoints, such as S/MIME for email encryption, and solutions that only protect certain parts of the transfer, such as SSL/TLS. Furthermore, there are some emerging, but as yet still rather scientific approaches that enable data to be encrypted during use, such as homomorphic encryption. The practical approach to protecting data in use at the application level builds on Format Preserving Encryption (FPE), data masking and on tokenization. While data masking can just replace some parts of the data such as certain fields or characters, tokenization uses one-way techniques to create a token for certain information that enables this to be used securely, without unveiling the original data. Tokenization typically delivers the advantage of dynamic data masking, which is display security, controlling what data or portion of data a user views as clear text, depending on their role in an organization. FPE uses standards-based encryption techniques, but delivers the encrypted result like a token, at predictable length, so that it can replace database entries without breaking the database schema.

Businesses face several challenges when looking for information protection based on encryption. Aside from the inherent complexity of encryption and the related technologies such as key management, tokenization, and data masking, there is no such thing as a single approach for all types of encryption. Frequently, business end up with a variety of point solutions, building distinct infrastructures per use

KuppingerCole Executive View
Vormetric Application Crypto Suite
Report No.: 79069



8 Page USL?
Jan20





2 Page A4
Jul-18
PLB7720

THALES

www.thalesecurity.com

WHEN THE MEDICAL INDUSTRY WANTS A REVIEW THEY CAN TRUST, ALLMED DELIVERS

Providing informed medical opinions is what physicians are paid to do. Each diagnosis and recommendation can trigger multiple outcomes, including prescriptions for drugs, insurance payment authorizations and formal completion of treatments. If a judgement is ever questioned or needs further validation a highly specialized category of company, known as an independent review organization (IRO), is called in to provide an expert review of the facts.

Headquartered in Portland, Oregon, AllMed Healthcare Management offers comprehensive physician peer review solutions to leading payer and provider organizations. The company utilizes a panel of hundreds of licensed, board-certified and actively practicing physicians to conduct its assessments. Their clients include medical management and managed care organizations (MMO, MCO), third party administrators (TPA) disability carriers and other providers.

Given the wide variety of highly confidential data that it handles, AllMed falls at the intersection of numerous federal, regional, industry and general regulatory mandates associated with personally identifiable information (PII), protected health information (PHI) and other sensitive data categories. As a demonstration of its commitment to adhere to the highest levels of data integrity, AllMed is one of just a handful of independent review organizations to have earned the stringent Health Information Trust Alliance (HITRUST) certification for information technology security.

BUSINESS NEED

Joel Campbell, Information Security Officer at AllMed, commented, "In the healthcare industry the number of regulations relating to data protection can be totally overwhelming, even for security professionals. For AllMed, being HITRUST certified is tangible proof to our stakeholders that we uphold the highest standards of security and privacy. They don't need to know what the 'HIPAA' or 'HITECH' acronyms stand for, they just need to know that we've met or exceeded industry-defined requirements relating to protecting patient data."

TECHNOLOGY NEED

HITRUST certification utilizes a comprehensive security framework that integrates requirements from many authoritative sources – such as ISO, NIST, PCI, HIPAA and others – and tailors them specifically to healthcare organizations. "HITRUST touches all aspects of an organization, so it is imperative to architect a solid foundation on which to build security policies, controls and procedures," reflected Campbell. "A key step was to ensure that our data is continually secure, and for me this means encryption."

He continued, "I've been in the security industry a long time and the number one name for encryption technologies has always been Thales. There are obviously competing products but Thales is always the name that jumps to the top."

"Without data integrity we wouldn't have a business. When prospects, or even existing clients, learn that we use Thales to perform our encryption duties, that's typically all they need to hear. They know we're serious."

"The number one name for encryption technologies has always been Thales. There are obviously competing products but Thales is always the name that jumps to the top."

– Joel Campbell, Information Security Officer, AllMed Healthcare Management



SOLUTION

AllMed deployed Vormetric Transparent Encryption from Thales in conjunction with the Vormetric Data Security Manager (DSM) to manage access policies and encryption keys across physical data centers, cloud environments and hybrid deployments. Vormetric Transparent Encryption provides the necessary access controls and data access logging functions needed by almost all compliance and data privacy standards and mandates, including PCI DSS, HIPAA/HITECH, GDPR and many others. AllMed is able to secure information with file and volume-level encryption for both data at rest and in motion. Agents installed above the file system on servers or virtual machines enforce data security and compliance policies, making deployment simple and fast.

"Everything gets encrypted," described Campbell. "HIPAA doesn't explicitly distinguish between different data states but by using Thales we immediately remove any concerns or issues about how we secure information."

RESULT

"We use a lot of different applications and were able to implement the Thales solutions without having to modify any code, databases or infrastructure components," recalled Campbell. "We have a modestly sized security team and despite serving such a critical role, the administrative overhead of the Thales solution has been phenomenally low, truly 'set and forget' once configured."

Providing its panel members with the information needed to review medical cases involves sending numerous files, some of significant size. This transfer process has several areas of potential vulnerability, especially because AllMed panelists are spread around the country, outside of the company's headquarters infrastructure. Campbell remarked, "With Thales we can prove that all data being transmitted is both unchanged and unseen, from its origin through to the receiving physician. Given its sensitivity, being able to guarantee that only the intended recipient can view the information is critical."

SERIOUS SECURITY

Campbell added, "AllMed is always looking for new business opportunities and we are growing quickly, making it essential that our IT infrastructure can support the company's business objectives. Thales has engineered its solutions to scale and adapt to accommodate exactly this type of dynamic situation."

The widespread, positive reputation of Thales continues to bring benefits, Campbell summarized, "Without data integrity we wouldn't have a business. When prospects, or even existing clients, learn that we use Thales to perform all our encryption duties, that's typically all they need to hear. They know we're serious."

BUSINESS NEED

- Create pervasive security for highly sensitive patient data
- Streamline compliance process across multiple regulations and mandates
- Support business agility and innovation with imposing restrictions or unnecessary overhead

TECHNOLOGY NEED

- Identify encryption solution to secure all sensitive information
- Secure data in all states and phases of transfer
- Assimilate easily into existing IT infrastructure without requiring widespread modifications

SOLUTION

- Vormetric Transparent Encryption from Thales
- Vormetric Data Security Manager from Thales

RESULT

- End-to-end data protection
- Attained HITRUST certification
- Deployment of Thales solutions used as a differentiator
- Adaptive infrastructure able to support dynamic business goals and growth objectives
- Nominal administrative overhead

ABOUT THALES eSECURITY

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premises, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

Follow us on:



Americas – Thales eSecurity Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4076 or +1 954 880 6500 • Fax: +1 954 880 6311 • E-mail: usa@thalessec.com
Asia Pacific – Thales Transport & Security (HK) Co., Ltd. 4011-3, 41/F, Sunlight Tower, 240 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 9633 • Fax: +852 2815 6141 • E-mail: asia.sales@thales-ess.com.hk
Europe, Middle East, Africa – Thales New Systems, Longwalk, Middlesex, UK • Tel: +44 (0)1844 200000 • Fax: +44 (0)1844 200550 • E-mail: emea.sales@thales-ess.com

© Thales - July 2018 • #187720

Case Study – Brother



2 Page A4
Dec-19
RMv9

thalesgroup.com

THALES

Brother Secures Employee Access and Reduces Costs with Cloud-based Authentication

Known for its sewing machines and printing solutions, the Brother Group secures access to its 24-hour IT support systems with cloud-based Thales SafeNet Trusted Access (formerly Gemalto SafeNet Authentication Service Cloud Edition). As a result, the company has experienced large-scale cost savings, reduced management loads, and guaranteed security of its core systems.

The Organization

Brother Industries Ltd. began with manufacturing and selling household sewing machines. Today, the company has locations in more than 40 countries, and sewing machines (including household and industrial machines) account for only 11 percent of sales, with approximately 70 percent from printing solutions, such as multifunction printers/fax machines.

The Business Need: Secure Remote Access

Brother Industries Ltd. has entrusted its information systems support to ABeam Consulting for many years. Together, they established a 24-hour support system comprised of approximately 30 staff, all equipped with secure computers for home use so systems could be accessed around the clock to maintain a high level of security.

The computers were equipped with identity checks, fingerprint authentication, and a troubleshooting system.

However, as end of support for Windows XP approached, Brother and ABeam Consulting had to examine other options, such as switching to Windows 7. Ultimately, they decided to replace users' computers with a thin client so that sensitive information would not be stored locally on PCs. At the same time, a switch to newer biometric authentication systems was examined. However, fingerprint authentication systems were infeasible so support technicians were sometimes unable to log into the system, which led to high help desk overhead. Brother needed an authentication solution that could guarantee high levels of security while also being low cost, easy to manage, and simple to use.



Challenge:

To enable secure remote access for the 24/7 support team, Brother required a cost-effective, agile authentication solution.

Solution:

Thales SafeNet Trusted Access (STA) verifies identities with cloud-based authentication and SMS one-time password authentication.

Benefit:

Team members can log in easily and securely, and Brother reduced operational costs by 40% by moving to a cloud-based solution.

The Solution: Cloud-based Authentication with SMS One-Time Password

Examination of the thin client and new authentication systems was started in September 2012. Brother chose T4U 2K as their thin client, which has a good balance between cost and function, and was already being used by other departments. To control access to the terminals, Brother evaluated a variety of two-factor authentication solutions, including traditional hardware tokens and SMS authentication. Hardware tokens were examined but rejected due to the cost of hardware, locale to users, and the need to replace lost tokens. Ultimately, Brother chose the Thales SafeNet Trusted Access (STA) one-time-password solution, a cloud-based method that authenticates by sending a one-time password to the user's mobile phone.

"Everyone has a cell phone, and we determined this to be both highly safe and simple because a password can be sent to a pre-registered email address," said Shigen Mizuno, Planning and Information Group 1 Manager, Strategic Promotion Department of Brother Industries. "Also, because the one-time password service is cloud-based, there is no need to set up a server, and startup is easy."

After two months of testing, Brother and ABeam moved the 30 support technicians to SafeNet Trusted Access. SafeNet Trusted Access makes strong authentication easy, offering flexibility to support all types of mobile phones and scalability to easily add users. SafeNet Trusted Access also provides completely automated processes and management functions, as well as customization, to allow for a seamless and comfortable user experience.

The Benefits: 40% Cost Reduction

Adoption of the new system resulted in large-scale cost reductions, as well as reduced operational requirements and expenses—approximately 40 percent savings. The simplicity of the login experience was well-received by the users, who appreciated the easy, reliable SMS authentication process. "Previously, we paid maintenance costs for the fingerprint authentication systems, as well as various operational burdens associated with the computers, such as added disk space, replacement of machines, and software and operating system updates. With the combination of the 2K thin client plus SafeNet Authentication Service, these costs have been rendered unnecessary, which is a great benefit. We believe that the new cost is roughly 60 percent of the previous system," said Mr. Mizuno.

While previous fingerprint scanners were temperamental, causing frustration and preventing users from logging into the system, the Thales one-time password solution using a cell phone

"With the combination of the 2K thin client plus SafeNet Authentication Service, we have eliminated many hardware and operational costs. We believe that the new cost is roughly 60 percent of the previous system."

— Shigen Mizuno, Planning and Information Group 1 Manager, Strategic Promotion Department of Brother Industries.

and the simple, easy-to-understand operation has been favorably accepted.

With the thin client, when system updates are necessary, all user environments are updated with one operation on the server side, which considerably reduces management operations. Also, Brother was able to integrate their existing VPN environment with SafeNet Trusted Access and the 2K thin client, reducing costs even further. Mr. Mizuno believes that "the results are above and beyond what we initially expected." Because of the resulting cost savings, reduced operating loads and simple, easy-to-understand operation, the system is now being examined for overseas expansion.

"Until now, support for overseas manufacturing and sales bases was conducted from Japan. However, if we use this system, we can entrust support duties to ABeam Consulting's overseas operation bases. We believe this can be handled locally. In the past, it was necessary to construct large-scale systems to ensure security over dedicated communication lines. However, with the thin client and Gemalto authentication, we are assured that our data remains secure," said Mr. Mizuno.

About Thales's SafeNet Access Management and Authentication Solutions


Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.


thalesgroup.com

Locations — Americas: Thales (USA) Capital of New York, New York, USA • Tel: +1 800 742 0270 • Fax: +1 212 267 2100 • Tel: +1 212 688 6211 • Email: sales@thales.com
Asia Pacific — Thales Security & Safety (P) L, 4/F, Gateway Tower, 300 Queen's Road East, Hong Kong • Tel: +852 2815 8622 • Fax: +852 2811 8140 • Email: sales.asia@thales.com
Europe, Middle East, Africa — Thales New York, Long Beach, Kentucky, United States • Tel: +1 858 424 2000 • Fax: +1 858 424 2001 • Email: sales@thales.com

© Thales - Dec 2019 - 2019







Colombia Secures Citizens' Access to Financial Services with Thales Strong Authentication

Challenge

In order to secure online access to national pension accounts and other services, FNA required a strong authentication solution with minimal infrastructural investment.

Solution

Thales (formerly Gemalto) SafeNet Trusted Access is a cloud-based solution, so FNA was able to easily and quickly roll out two-factor authentication for millions of users.

Benefit

Colombian citizens now enjoy the benefits of being able to access their pension accounts easily using SMS passcodes sent to their phones.

The Solution

In Thales, FNA found a solution that met all their requirements, plus extra benefits. Thales' SafeNet Trusted Access provides secure, cloud-based multi-factor authentication when Colombian citizens log into their FNA accounts. After entering their online user name and password, FNA account holders receive a one-time password (OTP) via SMS text or email that they then enter online as a second form of user authentication and additional security to protect their online accounts.


SafeNet Trusted Access delivers fully automated, highly secure and strong authentication with flexible token options that are tailored to the unique needs of each organization, substantially reducing the total cost of operation. With no infrastructure required, the service protects cloud-based and on-premise applications and data as well as corporate networks, identities and devices.

The Organization

Colombia's Fondo Nacional del Ahorro (FNA) is the Colombian Government Financial Institution established to facilitate loans to Colombian workers for home purchases. With more than 66 years' experience and 1.5 million users, the FNA operates to ensure the right of all Colombians to have housing and access to education. The FNA provides millions of citizens with a broad range of financial services, including retirement savings, loans, higher education financial support, and employment benefits.

The Business Need

In order to enable citizens to securely access its services, FNA required a strong authentication solution that could secure millions of users, and could be implemented quickly and easily without significant changes to infrastructure or up-front costs. In addition, FNA needed an authentication solution that was intuitive and easy to use for its citizens.



"We chose Thales because they are a leader in user authentication. Their cloud-based authentication solution met our goals to operate with no infrastructure costs and be highly automated. It was also very important that the SafeNet Authentication Service was very simple and easy to use for Fondo Nacional del Ahorro account users."

— César Amay, Vice President of Technology at FNA

The Benefits

As a cloud-based offering, SafeNet Trusted Access enabled the government of Colombia to rapidly deploy a highly scalable authentication solution to support millions of users with no upfront capital expenditures.

The FNA IT organization placed a high priority on ease of use, integration capabilities and cloud-based delivery. Thales' SafeNet Trusted Access integrated easily with the FNA back-office systems, which simplifies enrolling new users, provisioning new tokens, and reporting. Colombian citizens are able to easily understand and adopt Thales' intuitive authentication process, which provides one-time passcodes via the users' own SMS or email messaging services. "It was very important that the SafeNet Authentication Service was very simple and easy to use for Fondo Nacional del Ahorro account users," said César Amay, Vice President of Technology at FNA.

About Thales's SafeNet Access Management and Authentication Solutions

Thales' industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

2 Page A4
Oct-19
FRv4

© Thales. Document 2020 - FR v4.

thales.com

[LinkedIn](#)
[Facebook](#)
[Twitter](#)
[YouTube](#)

Americas – Mexico: Thales S, S de CV (Legal de Operaciones México) Calle 100, Avda. 10, 20131 USA • Tel: +1 800 340 3170 • +1 321 357 7200 • Fax: +1 321 358 0211 • Email: sales@thales.com
 Asia Pacific – Thales Network Security (P) L, 8th Floor, 4/F, Gateway Tower, 345 Queen Street East, Toronto, Ontario, Canada M5H 1H2 • Tel: +1 416 363 3833 • Fax: +1 416 363 3841 • Email: sales.asia@thales.com
 Europe, Middle East & Africa – Thales Network Security Limited, 100 Brook Street, London W1D 2LU, UK • Tel: +44 (0)20 7290 2000 • Fax: +44 (0)20 7290 2001 • Email: sales@thales.com



thalesgroup.com

THALES

Dudley Metropolitan Borough Council Cuts Costs by Switching to SafeNet Trusted Access

With local governments in the UK under the most severe financial pressures in living memory, yet at the same time needing to improve the services it provides to local taxpayers, Dudley Metropolitan Borough Council found that switching to Thales's SafeNet Trusted Access (formerly SafeNet Authentication Service (Cloud Edition)) lowers costs and demand on support staff by up to 30 percent.

The Organization

Dudley Metropolitan Borough Council is the governing body for the Dudley Metropolitan Borough in the West Midlands region of the United Kingdom. The Council represents more than 300,000 citizens and provides services such as roads and infrastructure, housing, schools, waste and recycling, libraries, social care, and community events.

The Business Need

Local governments in the UK are facing a perfect storm of spending cuts and pressure to improve the delivery of services. Remote working by council employees can help to deal with both of these imperatives, but providing a reliable security solution for remote access to council networks is in itself a significant expense, both in terms of the equipment needed and the staff

time required to manage it. Dudley MBC's network team was providing remote access for over a thousand users, but wanted to increase that number still further, enabling savings on office space and helping improve service quality. Its remote access infrastructure, though, was relatively costly and demanded a high degree of attention from technical staff.

The Solution

Thales (formerly Gemalto), along with its reseller partner Cision, agreed with Dudley to replace all of the council's 1150 remote access tokens, which had been supplied by rival firm RSA, with SafeNet Trusted Access tokens. Unlike the previous solution, the SafeNet Trusted Access tokens are sold on a pay-per-use licensing model. The agreement called for the replacement to be carried out over a three-year period. In fact, though, the migration process was completed in one year.

SafeNet Trusted Access delivers fully-automated, tightly secure and strong authentication with flexible token options that are tailored to the unique needs of each organization, substantially reducing the total cost of operation. With no infrastructure required, the service enables a quick migration to a multi-tier and multi-tenant cloud environment, and protects cloud-based and on-premise applications and data as well as corporate networks, identities and devices.

"We estimate we've saved 25-30 percent in support costs from implementing SafeNet Authentication Services. Increased enable working allows the authority to look at rationalising the office space it needs to provide, so the cost savings from the switch could potentially be much bigger over time. The great benefit was that there was no upfront cost for us. Whenever one of our old tokens expired, we bought a new one from Thales. And the licensing model means that, every time we replace a token, we're saving money."

-Adrian Turner, Network Unit Manager, Dudley MBC

The Benefits

Cost-Effective from Day One

Adrian Turner, Dudley MBC's network unit manager, says that SafeNet Trusted Access licensing model made the migration cost-effective from day one. "The great benefit was that there was no upfront cost for us," he explains. "Whenever one of our old tokens expired, we bought a new one from SafeNet Authentication Services. And the licensing model means that, every time we replace a token, we're saving money." Dudley's total IT user base incorporates around 5,000 desktops and 1,200 laptops. For a number of years, Turner says, the council has been trying to increase the mobility of its workforce, so five years ago, it partnered with a remote access provider to roll out a token-based system that would improve the security of its systems, as well as promoting home working. This system worked well, but Turner explains that he came to realize that a switch to SafeNet Trusted Access could improve functionality, as well as reducing the cost of operating the remote access infrastructure.

Lower TCO

"Our infrastructure was ageing, and required investment," he says. "We had 1,000 lay flats, and it was a monthly chore to replace them. Additionally, with SafeNet Trusted Access licensing model, the tokens don't expire after three years, leading to a significantly lower total cost of ownership. "SafeNet Trusted Access helped us build the infrastructure to support the migration," Turner explains. "It was very simple, and, with one engineer's help, we completed the job in half a day. We've had the odd teething problem, as you'd expect, but essentially it has been a very smooth process. We haven't had much need to call on further support - we've basically been able to handle it all internally." For a council like Dudley, cost is king - Turner says that the council is trying to cut £70 million from its budget over the next few years. "Every penny counts," he says. Increased mobile working allows the authority to look at rationalizing the office space it needs to provide, so the cost savings from the switch could potentially be much bigger over time.

Less Demands on Support Staff

But that isn't the end of the savings. The ease of use of the SafeNet Trusted Access tokens, by comparison with the previous system, means that Turner's team of engineers isn't needed to take as many support calls. "Our previous system was managed by my team," he explains. "We had network admins and technical engineers doing simple tasks like resetting PINs, because the front end was difficult for users to manage. With SafeNet Trusted Access, the front end is a self-web-based and intuitive, so we have passed that task over to our first line support desk, and we're getting very few calls to second line support. It's better for users too - for them, being dealt with by the support desk is quicker and better than having the job allocated to an engineer and having to wait for a response."

This too, Turner estimates, resulted in a 25-30 percent saving on support costs. When combined with the fee per cent Dudley is saving on lay flat purchases, it's no surprise that he, and his bosses, are happy with the switch to SafeNet Trusted Access. Now, the council is looking at further development of its remote access offering with SafeNet Trusted Access, including self-service options. In the present financial environment faced by local government, the sheer fact that Dudley is considering more developments is a real testimony to the success of SafeNet Trusted Access technology and business model.

Challenge

Dudley MBC is under pressure from its constituents to protect sensitive information while also cutting costs, but its existing RSA solution was expensive and cumbersome to manage.

Solution

SafeNet Trusted Access offers flexible licensing and pricing, so there are no upfront expenses, and the migration tool enables companies to manage both previous solutions and Thales tokens with one management console while easily moving users to Thales tokens.

Benefit

By switching to SafeNet Trusted Access, Dudley MBC not only implemented a leading remote access solution, but managed to cut costs and demand on support staff by up to 30 percent.

About Thales's SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

© Thales - November 2019 - ELCv10

thalesgroup.com

Amsterdam - Belgium: +31 (0)20 486 1111 | London: +44 (0)20 7175 1000 | New York: +1 (212) 257 2000 | Paris: +33 (0)1 41 00 00 00 | Rome: +39 (0)6 2611 0141 | Seoul: +82 (0)2 2011 0141 | Sydney: +61 (0)2 9211 0141 | Tokyo: +81 (0)3 4333 1000 | Washington DC: +1 (703) 441 2000 | Mexico City: +52 (0)55 5200 1000 | Sao Paulo: +55 (11) 3038 1000 | Lima: +51 (0)1 426 1000 | Bogotá: +57 (1) 261 1000 | Santiago: +56 (2) 2222 1000 | Lima: +51 (0)1 426 1000 | Bogotá: +57 (1) 261 1000 | Santiago: +56 (2) 2222 1000



2 Page A4
Nov-19
EHv3

thaligroup.com

THALES

Specsavers Brings Security into Focus with Thales Two-Factor Authentication

Challenge
A rapidly growing multinational retail chain, Specsavers needed an authentication solution allow its global workforce to securely access corporate resources and data.

Solution
They chose Thales (formerly Genetec) SafeNet Trusted Access with a mix of hardware, software and SMS tokens along with a tiered user-group structure allowing local management of the global solution.

Benefit
Specsavers now enjoys long-lasting hardware tokens, a scalable solution that will grow with the company, and lower total cost of ownership with Thales's unique OPEX payment model.

The Organization
Established in 1984 with two offices in the UK, Specsavers now has more than 1,300 branches and 26,000 staff across Europe, Australia and Asia. The eyewear company has firmly established a reputation for trust and value, and thrives on a joint-venture approach where the company and store directors work together in partnership, while managing a smaller number of wholly owned and franchised branches.

The Business Need
With a reputation for responding quickly to market opportunities, Specsavers is also quick to act when faced with risk and is conscious of the potential security issues that can affect a rapidly growing, multinational business. Specsavers currently has hundreds of remote users accessing a range of critical resources such as email, web applications and financial applications daily, and it aware that in order to ensure the security of its data, a data protection strategy was required.

Specsavers

"SafeNet Authentication Service has brought several benefits to Specsavers, the tiered usergroups have allowed us to implement and manage two-factor authentication globally, and delegate administration. The tokens work out to be cheaper and the technology offers us the highest level of security on the market. Feedback from our offices and end users has been really positive."
— Angus Dorsey, IT Security Manager at Specsavers



The Solution
With its dramatic growth, staff numbers continue to grow, so does the need for secure remote access. So Specsavers required a secure remote access solution that would be:

- Scalable and able to cope with the growth in staff levels across existing and new markets
- Flexible enough to suit different user working practices and technical capabilities
- Simple to administer
- Reduces the cost of implementation, deployment and ongoing resource requirements

Based on this criteria, Specsavers chose Thales SafeNet Trusted Access to secure remote access to their internal applications and databases. With SafeNet Trusted Access, Specsavers is now able to deploy authentication tokens to users globally and on demand through the unique tiered user-group structure. By creating groups within the SafeNet Trusted Access management portal to represent each location, Specsavers' Head Office is able to pass management of each group to a local administrator.

Specsavers chose a mix of token formats: hardware, software and SMS, to meet various end user needs. The tokens, combined with a unique PIN code, deliver a one-time password (OTP) which can include letters, numbers and characters, offering the most secure OTPs on the market. When the user enters the correct PIN and OTP to the Specsavers remote gateway, they are securely authenticated and granted access to the server. With SafeNet Trusted Access in place, Specsavers has enabled its mobile and remote users to easily connect to the company's resources and applications securely.

The Benefits
SafeNet Trusted Access has enabled Specsavers to secure employees remote access to its internal applications and databases, and brought numerous other benefits including decreased costs.

Scalability and Empowerment. The tiered user group function eases the burden on Specsavers' central IT department, and empowers local offices to instantly allocate and retract tokens as required. SafeNet Trusted Access is the only vendor with this level of functionality. For Specsavers, this means they can benefit from the economy of scale of having one global service, instead of having to purchase and manage a different server in each location.

Token Longevity. Previously, Specsavers had found hardware tokens to be unreliable and frustrating as the token expired within three years. This time, the company chose a mix of hard, soft and SMS tokens. The software tokens are most suitable for users with access to a single desktop or laptop, the SMS tokens are deployed for users who require portability, and users preferring a hardware token have been issued with hardware tokens. Soft and SMS tokens significantly reduce token costs, additionally the hardware token has a 5-year warranty and no expiration date, and should a battery run out they are easy for the user to replace.

Lower TCO. Specsavers have confidence in SafeNet Trusted Access simple annual subscription fee which includes the service's software components and applications. With this OPEX model, the company has been able to eliminate the hassle and cost of up-front investment in software and hardware, and by taking the complexity and cost out of implementation and ongoing support, SafeNet Trusted Access has enabled Specsavers' IT staff to focus on more profitable activities. As Angus Dorsey, IT Security Manager of Specsavers confirms, "We have been using SafeNet Authentication Service for over two years now, and have yet to replace a single token or battery. There are obvious cost and resource savings for us when using reliable long-life tokens and we are already seeing those benefits."

About Thales
The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

thaligroup.com • • info@thaligroup.com
 Americas - Mexico Plaza 1, 1440 Capital of Texas Highway North, Suite 100, Austin, TX 78701 USA • Tel: +1 800 240 5170 • +1 512 357 2900 • Fax: +1 514 888 6271 • E-mail: info@thaligroup.com
 Asia Pacific - Thales Telecom & Security (P) L, 401, 401, 401, 401, Singapore, 240 Queen's Road East, Hong Kong • Tel: +852 2815 8622 • Fax: +852 2815 8141 • E-mail: info.asia@thaligroup.com
 Europe, Middle East, & Africa - Avenue des Nations, Long Champs, 92084 Nanterre Cedex, France • Tel: +33 (0)1 47 35 10 00 • Fax: +33 (0)1 47 35 10 01 • E-mail: www.asia@thaligroup.com



2 Page A4
Nov-19
RMv7

thalesgroup.com

THALES

Thales's SafeNet Trusted Access Helps Prevent Employee Identity Theft at VUMC

Plagued with phishing emails almost daily, this Nashville-based medical center at Vanderbilt University decided to add an extra layer of security by leveraging multifactor authentication within their organization. With the help of Thales (formerly Gemalto), VUMC can thwart cyber criminals' attempts at stealing sensitive data.

The Organization

Managing more than 2 million patient visits annually, Vanderbilt University Medical Center (VUMC) in Nashville, Tennessee, is one of the largest academic medical centers in the southeast U.S.A.

The Business Need

According to VUMC, cyber criminals had been targeting this healthcare institute to steal employee login credentials and then try to enter C2HR, the center's self-service human resources portal. Human resource departments are a favorite among thieves, because that is where a lot of the most delicate employee data is held. The most common tactic in this institute was email scams where imposters sent phishing emails, posing as VUMC employees. With employees' email login credentials, hackers can access the human resource departments and attempt to get hold of their bank account information, automatic deposit of paychecks information, and social security numbers.

Challenge

- Vanderbilt University Medical Center sought an effective MFA solution that would prevent unauthorized access to employee credentials and thus minimize risk of manipulating these credentials to commit fraud, such as phishing attacks.

Solution

- SafeNet Trusted Access (formerly SAS Cloud), Thales's cloud-based Authentication Solution was chosen, along with SafeNet MobilePASS, to support both software and hardware options for their employees' varied network access devices.

Benefits

- Deploying the solution has enabled the medical institute to protect employee data integrity, enable stronger access to systems and resources, and prevent security breaches.



"We're beginning the switch to broad use of multi-factor authentication as an important new safeguard for our employees and our enterprise. Security attacks are unrelenting, and we view MFA as a vital and necessary addition to VUMC's enterprise cybersecurity program."

— Andrew Hutchinson, Executive Director, of Enterprise Cybersecurity, VUMC.org

The enterprise cybersecurity unit of VUMC in Nashville detected phishing emails being sent using stolen or fake names of employees. VUMC noted that since 2016, the volume of phishing emails increased in the top five targeted industries, including healthcare, by about a third. These attacks coincide with figures reported by Gemalto's breach level index H1 2018 report – Healthcare companies experienced the greatest amount of security events in the first half of 2018, amongst all the industries. Thales also explains that the larger ramifications of data breaches is often unknown, as hackers use stolen data to orchestrate other attacks.

With sensitive and confidential data being endangered on a daily basis, VUMC needed a method to add another layer of security to make sure that only authorized people accessed certain resources. The medical institute needed to put an end to the theft of employee credentials, as the first step to minimize security breaches. Preventing corporate identity theft also mitigates the risk of cyber criminals being able to use these credentials to carry out phishing attacks and potential financial and reputational damage to the institute and its employees. Multi-factor authentication requires that users must provide something more than (or stronger than) a password to log into a system. Using a second factor or third factor of authentication, employee credentials are much harder to seize.

The Solution

VUMC now utilizes Thales's SafeNet Trusted Access, Thales's cloud-based Authentication Solution and SafeNet MobilePASS. As of November 19, 2018, VUMC requires multifactor authentication when users of the self-service portal of the university medical center's human resource center try to access their direct deposit details, tax information or personal profile. This capability was provided by an app called SafeNet MobilePASS, which can be downloaded to most mobile devices. Users without a smart phone can use a hard token with a digital readout for display of authentication codes.

Multifactor Medicine in Nashville: Thales's SafeNet Trusted Access

SafeNet Trusted Access leverages the authentication methods already employed in an organization's cyber security program. Switching to a broader practice of multi-factor authentication safeguards access to sensitive information. This is done by replacing a static password with a second factor of authentication that cannot be hacked or stolen. SafeNet Trusted Access supports a large variety of form factors and authentication methods to allow VUMC stronger authentication and more secure access to effectively manage risk.

The Benefits

Benefits for VUMC

- Prevent security breaches: SafeNet Trusted Access mitigates risk associated with identity thefts. With additional factors of authentication required when users access sensitive resources, the medical institute can reduce risk of compromised data records, protect the integrity of their systems and prevent potential threats and security breaches.
- Provides flexible form factors for diverse use cases: SafeNet Trusted Access supports both software and hardware authenticators. Thales offers VUMC whichever option their employees require, depending on the device they use to access their systems. System users with mobile phones can receive multi-factor authentication codes via a smartphone app or SMS text message. Users without a mobile phone can use a hard token that displays their authentication codes digitally.
- Leverage MFA throughout the enterprise: To comply with DEA rules for electronic prescribing of controlled substances, VUMC deployed MFA with a Thales SafeNet system in November, 2017. A year later, VUMC has implemented SafeNet Trusted Access for HR portal purposes. VUMC is leveraging the success of MFA for other areas. According to Andrew Hutchinson, executive director of Enterprise Cybersecurity at VUMC, 'additional VUMC systems will begin to require this form of user authentication'.

A more secure future

VUMC mission statement states that Vanderbilt aims to 'combine their transformative learning programs and compelling discoveries to provide distinctive personalized care'. Thales's SafeNet solutions assist Vanderbilt in managing, protecting and caring for the users involved in this mission, helping to ensure that their data remains in the hands of authorized users only.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> thalesgroup.com <

Amman - Adnan Plaza 3, 9442 Capital of Iraq Highway North, Suite 100, Amman, 767019 USA • Tel: +1 888 343 5773 • Fax: +1 512 257 3900 • Email: sales@thales.com
Asia Pacific - Thales Transport & Security (HK) Co., Ltd. 41/F, 3, Sunlight Tower, 248 Queen's Road East, Hong Kong • Tel: +852 2915 9833 • Fax: +852 2915 9840 • E-mail: asia.sales@thales-security.com
Europe, Middle East, Africa - Meadow View House, Long London, Aylesbury, Bucks HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 206550 • E-mail: sales@thales-security.com

© Thales - November 2019 • RMV7



2 Page A4
Dec-19
RMv9

thalesgroup.com

THALES

Westcon Relies on SafeNet Trusted Access for Constant Uptime and Reduced Costs

Norwegian shipyard Westcon requires robust authentication to support 700 users, some of whom access the corporate network from offshore oil rigs and vessels. A switch to SafeNet Trusted Access [formerly SafeNet Authentication Service - SAS Cloud] improved reliability and reduced costs.

Background

Based in the small town of Ølavså, the Westcon shipyard is located on the west coast of Norway, not far from the city of Stavanger, the centre of the country's large oil industry. The yard specialises in the construction and repair of both ships and oil rigs. The company has grown significantly in the last decade, becoming one of the most modern and successful offshore and maritime service facilities in the industry.

Business Need

Westcon's IT network covers over 700 users, with many needing to access corporate systems from off-site, sometimes even from offshore rigs and vessels. To support these remote users, the company had put in place an authentication system, but, according to IT Manager Kjell Thorsen, the system had its problems. "From time to time, we would have troubles with the authentication system, in particular, we had too much downtime," he says. "Our IT department is small – we only have seven people to support the

entire corporate IT infrastructure – and we don't have the resources to deal with these kinds of problems. For that reason, we determined that we wanted to switch to a hosted solution for authentication, and that was what led us Gemalto."

Challenge

With many employees remotely connecting to corporate resources – including offshore oil rigs and vessels – Westcon required strong authentication to verify identities of those accessing sensitive material. But their existing solution proved problematic with frequent downtime and lost productivity.

Solution

Westcon chose to move to SafeNet Trusted Access, a hosted solution, which provides Westcon with 100% uptime. It also interfaces with existing tokens so Westcon is able to manage its existing hardware and new SMS tokens in one userfriendly platform.

Benefit

With SafeNet Trusted Access, Westcon preserved its investment in existing hardware tokens, while moving to a reliable, easy-to-use management platform featuring 100% uptime and simplified maintenance that meets their stringent security needs, as well as an Op-Ex payment model that fits their budget.

WESTCON®

"We don't have worry about uptime – the system is always up and running, and if we ever do encounter a problem, we have strong and reliable partners who we know will resolve it very quickly."

– Kjell Thorsen, IT Manager, Westcon

Solution

Thorsen and his team engaged with Thales (formerly Gemalto) to investigate which of its market leading authentication solutions were the best fit for Westcon's needs. Based on the requirements specified by Westcon, Thales recommended a switch to its SafeNet Trusted Access. Westcon also implemented SafeNet SMS token technology, which delivers a one-time access code to a mobile phone by way of a text message, and thus enables authentication in almost any circumstances.

"Gemalto was of great help to us," says Thorsen. "They introduced us to the SafeNet Authentication Service option, and it quickly became clear to us that Gemalto's technology was the best option for our needs." The fact that the SafeNet Trusted Access delivery model means no upfront costs was even better news, he adds. Since SafeNet Trusted Access supports third party tokens for authentication, Westcon did not lose any of its investment in the previous solution, as users continued to authenticate with their existing tokens until those expired. The self-service aspect of SafeNet Trusted Access meant that users are able to deal with most problems that arise themselves, reducing the need for helpdesk services.

Benefits

Now, Westcon is using SafeNet Trusted Access to provide authentication for more than 120 remote users. "The best thing of all is that we have a 100 per cent stable authentication solution," says Thorsen. "We don't have worry about uptime – the system is always up and running, and if we ever do encounter a problem, we have strong and reliable partners who we know will resolve it very quickly."

As SafeNet Trusted Access is fully automated, including user set-up and provisioning automation, the load of Thorsen's team has been reduced too. The process of migrating to the Thales solution, he says, was straightforward and handled effectively by the team from Thales, with no impact on the company's remote users out in the field. And on top of that, Westcon is saving money. "We have been using the Gemalto solution for around eighteen months now, and although cost was not our main priority, we are spending less on authentication than we were with our previous vendor," says Thorsen. "I would recommend a switch to cloud-based authentication – and Gemalto – for many companies. The reduction in management work alone is very valuable, but when the other benefits of Gemalto authentication are added to the mix, then it becomes a very easy decision to make."

About SafeNet Trusted Access

SafeNet Trusted Access is a cloud-based access management service that combines the convenience of cloud and web single sign-on (SSO) with granular access security. By validating identities, enforcing access policies and applying Smart Single Sign-On, organizations can ensure secure, convenient access to numerous cloud applications from one easy-to-navigate console.

Strong authentication is made easy through the flexibility and scalability of SafeNet Trusted Access's automated workflows, and vendor-agnostic token integrations and broad APIs. In addition, management capabilities and processes are fully automated and customizable – providing a seamless, and enhanced, user experience. With no infrastructure required, SafeNet Trusted Access enables a quick migration to a multi-tier and multi-tenant cloud environment, and protects everything, from cloud-based and on-premise applications, to networks, to users and devices.

About Thales's SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> thalesgroup.com <

Americas – Ardmore Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5373 or +1 512 257 3900 • Fax: +1 954 886 4201 • E-mail: sales@thalessec.com
Asia Pacific – Thales Transport & Security (HK) Ltd, Unit 4101-3, 41/F, Sunlight Tower, 240 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8941 • E-mail: asia.sales@thales-sec.com
Europe, Middle East, Africa – Alandow New House, Long Crossin, Aylesbury, Buckinghamshire HP18 9EG • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 206550 • E-mail: amea.sales@thales-sec.com

© Thales - December 2019 • RMV9



2 Page A4
Oct-19
RMv3




Industrial Company Triumphs with Flexible Access Security, Thanks to SafeNet Trusted Access

When this industrial enterprise decided to migrate to Microsoft Office 365 in the cloud, they assumed that they were protected. However, they found out the difficult way that only a stronger authentication and access management solution could provide them with more effective security.

Industry Overview

Industrial organizations produce merchandise by transforming raw materials into finished products, sold on a large scale. The product lifecycle spans numerous networks and groups of users, from wholesalers through retailers and consumers. It is not just physical resources that are refined, but also digital assets containing confidential information.



SafeNet Trusted Access

- Streamline security
- Enable cloud transformation securely
- Simplify compliance

The Business Need

A large industrial company approached Thales after experiencing a security incident that occurred when it moved to Microsoft Office 365. Although using web-based apps such as Office 365 has become standard practice for many enterprises, this company moved to the cloud without implementing any robust 2FA authentication method.

And as one particular industrial company with thousands of employees discovered the hard way, the process of migrating to the cloud is critical. According to a Breach Level Index 2018 report, the industrial sector saw the highest growth rate of data breaches among all other sectors.

Challenge

To avoid such breaches, the company sought to implement a secure Access Management solution, with strong 2FA authentication and role-based access policies. Like many industrial enterprises, the company works with different types of users who have different needs, and sought an access management solution that could support a range of authentication methods.

Solution

After assessing several Access Management solutions available on the market, the company chose to implement SafeNet Trusted Access from Thales.

Benefits

SafeNet Trusted Access made it easy to implement secure access and strong authentication with Microsoft Office 365, offering robust application protection that is convenient for end-users. Added value was low TCO due to inclusive hardware and software-based tokens, all in one license.



Solution

After assessing several Access Management solutions available on the market, the company chose to implement SafeNet Trusted Access. SafeNet Trusted Access makes it easy to implement Access Control and Strong Authentication with Microsoft Office 365, offering robust application protection that is convenient for end-users. This Access Management solution offers flexible access management through a simple to use policy engine that gives customer real-time control over the ability to enforce policies at the group or application level. The Access Management service helped secure secure and convenient access to Office 365 environment depending on employees' context.

2FA Required for Office 365 App.



A critical factor in the decision to select SafeNet Trusted Access was the fact that it offered a range of different authentication methods as part of its basic license, at no additional cost, enabling it to address different population groups with a single solution.

In this way, the employees equipped with a corporate mobile phone used a software phone-based token to authenticate through a simple push notification on their mobile phones. The other employees used a hardware token, which permitted them to authenticate via OTP. Contractors without corporate devices were able to authenticate flexibly to the pattern-based software token called CellDance.

Pattern-Based Authentication for Contractors



Benefits

Flexible Business Model

By providing software and hardware tokens included in the SafeNet Trusted Access license, the company was able to deploy a single solution that met all of its needs, significantly reducing TCO.

Data Breach Prevention

With secure access management in place for their cloud-based apps, the company can adopt more web and cloud-based apps in the future and mitigate risk of future corporate identity theft and phishing attacks.

Enhanced User Convenience

Thales was able to offer a choice of authentication options that met users' expectations for security and convenience.

About Thales's SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.



© Thales, October 2019 • RMv3



2 Page A4
Jun-19
GHv5

thalescpl.com

THALES

Law Firm lifts the Fog over Cloud App Security with SafeNet Trusted Access

Overview

Lawyers typically have very specific IT needs and user experience is key. As a niche industry, security is critical to their business survival. The danger of cyber-attacks is real. The FBI has been warning about impending attacks for a few years. With the growing number of cloud applications, it's no longer enough to secure in-house, on-prem applications, many law firms work remotely with both clients and regulatory bodies – using cloud and web-based applications or integrated cloud applications, such as (but not limited to) Salesforce, AWS and Citrix.

Apart from potential financial and reputation damage, the drivers for law firms to manage access to their applications, there are regulatory drivers as well. For example, GDPR and U.S. law may require firms to notify both clients that they represent and regulators if they suspect a data breach of personal data.

According to LOGICFORCE and an ABA Technology Survey, 22% of law firms were attacked in 2017, up 14% from the previous year. One of the reasons these firms are particularly vulnerable to breaches is because many do not invest the money to properly secure their data.

Challenge

In light of increasing regulations and the need to protect their growing number of cloud and web-based applications, a law firm approached Thales to inquire about their new Access Management solution – SafeNet Trusted Access. The law firm was an established customer and was already using Thales's SafeNet Authentication Service installed in on-premises. However, they wanted to extend protection to their cloud applications without increasing the login burden for their staff. The organization was looking for a solution that could offer flexible policies which could differentiate between trusted and risky networks.

“Contextual logging in from within and outside the office was really important to us. With SafeNet Trusted Access, we enjoy great user experience with push authentication and SSO.”
– Security Officer, Law Firm

The Solution

Thales's SafeNet Trusted Access offered the law firm simplified cloud access with Single Sign On (SSO) secured by contextual access security. The Access Management Service provides privileged access policies for senior partners, financial officers or other executives. Policies can be set up per role, i.e. paralegal or clerk, who will not need access to sensitive applications.

Context-sensitive SSO

SafeNet Trusted Access combines the convenience of single sign-on with context-sensitive access security. By validating identities, the solution helped the law firm ensure secure, convenient access to all their cloud and web-based applications. Smart SSO let the law firm employees and contractors log in to all their cloud applications with a single identity, and only requires them to provide additional authentication in high risk login situations. Depending on their role or location, users are required to provide additional authentication or less restrictive steps, as required by the access policies. In this way, users may authenticate just once in order to access all their cloud applications, or provide additional authentication, as required by the policy.

Benefits

Thales's SafeNet Trusted Access provided the law firm with the level of security they required as well as flexible access management policies. These included different policies based on role, context or location. For example, it was very important for the law firm to mitigate high and low-risk cases, inside the office (trusted networks) and outside the office (higher risk networks).

SafeNet Trusted Access allowed the law firm to integrate with more cloud applications as the company expanded, and restrict or alleviate authentication as needed, to workers and contractors across the legal ecosystem.

About SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

To learn more about access management from Thales,

visit <https://safenet.gemalto.com/access-management/> or join a live demo webinar at <https://www.brighttalk.com/webcast/2037/334449>.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Policies in SafeNet Trusted Access for users working remotely or from trusted networks



Thales © 2020 All rights reserved.

> thalescpl.com <



Amsterdam – Thales Group Inc. 2360 Junction Ave, San Jose, CA 95134 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thales.com
Asia Pacific – Thales Trustgate & Security (P) Ltd, Unit 4102-3, 42/F, Sunlight Tower, 243 Queen's Road East, Hong Kong • Tel: +852 2315 9633 • Fax: +852 2315 9341 • E-mail: sales.asia@thales.com
Europe, Middle East, Africa – Thales Trustgate & Security, London, United Kingdom, Brickley Walk, London E15 1JG • Tel: +44 (0)204 201600 • Fax: +44 (0)204 206550 • E-mail: sales@thales-security.com

© Thales-June 2019 • GHv5



thalescpt.com

THALES

Real Estate Development Company Ensures Secure Cloud Access with Thales's SafeNet Trusted Access

Overview

An international real estate development company wanted to offer employees a convenient way of working remotely by easily and securely accessing the corporate network as well as cloud and web-based applications.

Concerned with the rising number of security breaches, the company at first, considered applying strong authentication for each application. They dismissed this solution however, since it would require their employees to login with a second factor of authentication for each app – which they felt would inconvenience their employees. As the company expanded its cloud transformation initiative, the issue of security and convenience became more urgent, and they sought a solution that could provide both user convenience and secure access to corporate apps.

Challenge

Prevent cyber-attack without losing productivity

The company chose Thales's SafeNet Trusted Access to address their need for a convenient and secure login experience.



"The most important factor for our organization was the fact that SafeNet Trusted Access enabled us to offer a convenient and simple user experience for our employees. Thales met this need, creating excellent value."
– IT officer, Real Estate Company

The need for access management in the Real Estate Sector

With the increase in adoption of cloud applications in enterprises worldwide comes the increase in risk of cyber attacks. The cost of an attack is not just damaged reputation, but also financial loss. The real estate industry is just as vulnerable. However, encrypting or securing data is only one part of cyber security. Real estate companies need to control the access to their data so that only the right people get hold of the right data in the right applications at the right time.

The Solution

SafeNet Trusted Access provided the real estate company with a policy-based access management service which offers both MFA and the SSO experience they were seeking.

Easily secure and manage access with a single cloud service

SafeNet Trusted Access lets organizations easily secure and manage access to web and cloud apps with a single cloud service. The solution made it easy and convenient for the company's users to access all their apps with by letting them log into multiple cloud and web apps once, and provide additional step up authentication only when needed.

The solution lets organizations leverage their inherent authentication methods and add new apps to existing policies, or configure new ones as needed. The priority was to provide a single-sign on experience to their end users, while still being able to require stronger methods of authentication for more sensitive apps. The organization was able to deploy SafeNet Trusted Access for SAML-based apps and use second factor authentication via its built-in SafeNet Authentication Service for Radius applications.

Benefits

After implementing SafeNet Trusted Access, the company could centrally manage access for several apps that are deployed in their organization and allow users to log in to cloud and web apps without having to reauthenticate each time. Thales's SafeNet Trusted Access provided the organization with one solution that supported the majority of its applications while providing an extra layer of security for the sensitive ones. With SafeNet Trusted Access, the organization gained smart SSO that combines multifactor authentication together with convenient single sign on for a more productive yet secure work experience.

Second factor authentication policy for High Risk users



Single Sign On Policy for Low Risk Scenario in SafeNet Trusted Access



About SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy-based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

To learn more about access management from Thales,

visit <https://safenet.gemalto.com/access-management/> or join a [livedemo webinar at https://www.brighttalk.com/webcast/2037/334440](https://www.brighttalk.com/webcast/2037/334440)

About Thales Cloud Protection & Licensing

Today's enterprises depend on the cloud, data and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored – from the cloud and data centers to devices and across networks. Our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.

> thalescpt.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • Email: sales@thalessec.com
Asia Pacific – Thales Transport & Security (HK) B, Unit 4101-3, 41/F, Sunlight Tower, 348 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 6361 • Email: cna.sales@thales-sec.com
Europe, Middle East, Africa – Thales UK eSec, Longwalk, Middlesex, Uxbridge, Middlesex UB8 3PH UK • Tel: +44 (0)1844 205100 • Fax: +44 (0)1844 205550 • Email: www.sales@thales-sec.com

© Thales - June 2020 - GH v6

2 Page A4
Jun-19
GHv6
(accompanies
video)



Visit our Thales End User BrightTalk Channel

➤ [Thales CPL On BrightTalk](#)

End Customer

- [Webinar: Best Practices for Securing Access to Office 365](#)
- [Webinar: Global Trends in Cloud Access Management, Single Sign On & Authentication](#)
- [Webinar: Identities Are the New Security Perimeter in a Zero Trust World](#)
- [Webinar: Global Trends in Cloud Access Management, Single Sign On and Authentication](#)



Visit our Thales Partner Only Tech Talks

- [Partner Tech Talks - Live Webinars](#)
- [Partner Tech Talks - On Demand Catalogue](#)

Thales Access Management Webinar for Partners

- INTERNAL : PARTNERS ONLY
- Identities are the new security perimeter in a zero trust world: Use them effectively to secure your distributed IT environment. Partners are invited to Join Ashley Adams, Access Management Product Marketing Manager to learn how identities are becoming the new security perimeter in a zero trust world and present best practices for implementing an access management framework that can help organizations remain secure – and scale – in distributed networking environments.

SafeNet Trusted Access Value Proposition

- INTERNAL : PARTNERS ONLY
- Join the Thales Identity and Access Management team for their Coffee Break Video featuring Ashley Adams, Product Marketing Manager chatting with Gemma Ainsley, Channel Marketing Manager, about a current hot topic for partners. The format is short – just enough time for a coffee break – and conversational, which makes it seem like you are simple part of a smart conversation. In the chat, we outline the core messages and value proposition of SafeNet Trusted Access (STA). Listen in on this short conversation to increase your knowledge of the product and gain some insights on how to better pitch SafeNet Trusted Access (STA). Grab a cup of coffee, tune in and enjoy!



O365 Integration



➤ https://www.youtube.com/watch?v=E4PyQvdv_Pc

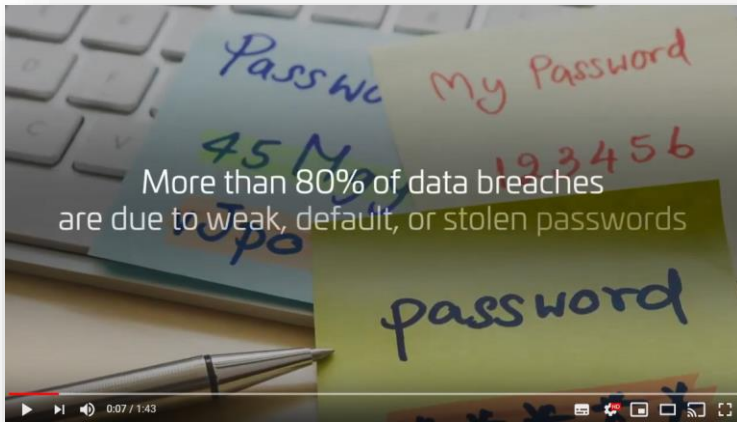
Simple SSS vs Smart SSO



➤ <https://www.youtube.com/watch?v=vslXudnSSX8>



Passwordless Authentication Solutions by Thales



- *** NEW ***
- https://www.youtube.com/watch?v=kGxhK50W7_I&feature=youtu.be

SafeNet Trusted Access from Thales



- <https://www.youtube.com/watch?v=RXIJCSpa5n4>

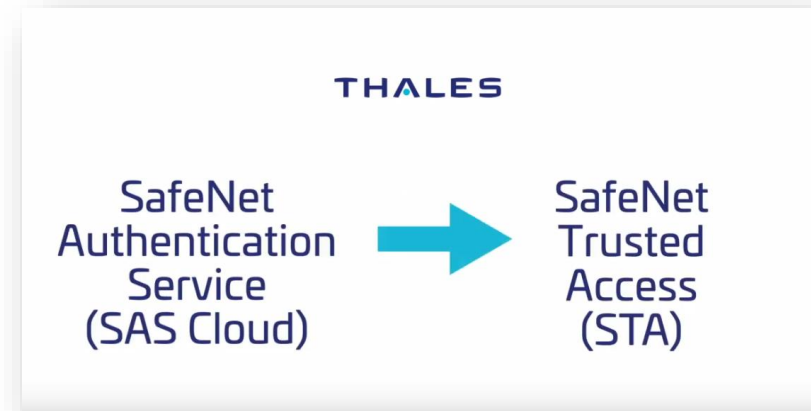


How Access Management enables Cloud Compliance | SafeNet Trusted Access | GDPR, HIPAA, PCI DSS



➤ <https://www.youtube.com/watch?v=kBsy-JT0VIk>

SafeNet Trusted Access Basic (STA Basic)



➤ <https://www.youtube.com/watch?v=W0W4X1jDIBg&t=16s>



MS Azure AD Demo



➤ <https://www.youtube.com/watch?v=6B86JMqzYGI>

Retail Example Demo



➤ Received files



Real Estate Case Study



STA CIAB
EDM1

➤ https://youtu.be/rf_HuT0Gcg8

VU Medical Centre Case Study



➤ <https://www.youtube.com/watch?v=oNY82E1A01A&feature=youtu.be>



Microsoft

	AAD 2019 new features by Gil mazor	20/01/2020 08:26	Microsoft PowerP...	9,636 KB
	Best practices for securing 0365 - with detailed notes for sales - internal or partner	20/01/2020 08:26	Microsoft PowerP...	3,343 KB
	best practices for securing 0365 with Thalès AM and MFA - customer facing	20/01/2020 08:26	Adobe Acrobat D...	1,577 KB
	how Azure MFA has weak HW OTP token management_November	20/01/2020 08:26	Microsoft PowerP...	1,079 KB
	Microsoft Competitive Analysis_Battle Card Jan 2020	20/01/2020 08:27	Microsoft PowerP...	2,426 KB

DUO

	Audio sales elevator pitch duo security	20/01/2020 08:19	MP3 Format Sound	2,695 KB
	Competitive Workshop - Duo functional and technical analysis - June 2019	20/01/2020 08:13	Microsoft PowerP...	2,756 KB
	DUO Battle Card August 2019	20/01/2020 08:14	Adobe Acrobat D...	500 KB
	DUO detailed competitive analysis August 2019	20/01/2020 08:16	Microsoft PowerP...	3,963 KB
	DUO vs STA features comparison-August 2019	20/01/2020 08:18	Microsoft Word D...	30 KB

BATTLE CARD – SafeNet Trusted Access vs Duo Access

6 Ways STA is better than Duo

- Lower Total Costs of Ownership
- Easier to deploy
- Support more use cases
- Broader MFA options
- More flexible policy engine
- Superior Reporting

Why Thalès?

- More than 30 years of experience in protecting digital identities
- More than 25,000 IAM customers and over 30 million users
- First IAM vendor to offer a cloud-based MFA service

Duo Weakness	Details
1. High TCO	<ul style="list-style-type: none"> Expensive license HW token priced on top multiple on-prem components - hybrid architecture means higher overheads
2. Complex deployment	<ul style="list-style-type: none"> Duo is script based, hard to configure Requires installation of multiple on-prem components
3. Limited use cases	<ul style="list-style-type: none"> Does not support OIGC or Kerberos
4. Limited MFA options	<ul style="list-style-type: none"> No native HW tokens, no email OTP, no pattern-based tokens, no CBA, limited biometric
5. Complex policy set up	<ul style="list-style-type: none"> Each app needs its own policy pwd authentication is not available in policy engine
6. Limited reporting	<ul style="list-style-type: none"> Only 10 reports No integration with SIEM

Planting Landmines

Questions to ask customers who are considering Duo

- High TCO**
Do you plan to use DUO to protect network, VPN and on-prem apps?
Are you aware of the EXTRA overheads that requires?

Duo Licenses are expensive:

- Duo MFA:** \$5/um has limited functionalities. It offers only basic SSO, limited conditions, no HW token, limited support for on-prem apps
- Duo Access:** \$5/um; limited support for on-prem apps
- Duo Beyond:** \$9/um

DUO is NOT a 100% cloud solution: It requires installing and maintaining multiple on-premises components on a Linux or Windows machine. These include:

- Duo **Access** Gateway (DAG) to support 1st factor authentication (Active Directory username, password) and to support remote network (VPN) access.
- DUO **Authentication Proxy** to support LDAP authentication for non-web resources (e.g. clients).
- DUO **Network** Gateway (DNG) to support internal on-prem portals, e.g. Confluence, Jira, SharePoint (part of Duo Beyond license)

Two servers **add** a load balancer in front of **each** of the above (DAG, DNG, Auth Proxy) to ensure HA and redundancy. **This means up to nine (9) servers to manage on-premises!**

STA delivers **built** RADIUS-as-a-service and SAML-as-a-service, entirely managed in the cloud. You get the flexibility to deploy as you like at a much better TCO.

Planting Landmines

Questions to ask customers who are considering Duo

- Complex to deploy**
When do you plan to be up and running?
Duo's Synchron agent and Auth proxy are script based - not easy or convenient to use
- Limited use cases:**
do you have on-prem apps that do not support SAML?
Do you want to implement SSO after windows login?
- Limited MFA**
What type of MFA tokens do you plan to use? For which type of users?
Are you concerned about data breaches?

- With Duo, you can only support on-prem web apps with SAML (no OIGC)
- You'll need Duo Beyond to protect on-prem apps without a VPN. STA can do this by integrating out of the box with all leading reverse proxies.
- With Duo you can not manage SSO after windows login (no Kerberos)
- DUO provides limited MFA functionalities: no pattern based token, no CBA, no Email OTP, no native hardware tokens. These are only available by integrating 3rd party tokens.
- Duo Mobile passcode does not support TOTP token drift or TOTP resync. As a result, TOTP tokens may eventually fall out of sync and generate invalid passcodes.
- Duo tokens can be backed up to Google drive which means they are less secure

STA delivers standards-based security with secure protocols & workflows, and high assurance tokens.

Planting Landmines

Questions to ask customers who are considering Duo

- Complex Policy set up**
How do you plan to manage policies in DUO?
In Duo, no central policy configuration for all apps. Policy has to be configured and then applied separately to each app. This can double the time to set up a policy in certain scenarios (e.g. applying policy to privileged user group, denying access from certain countries).
In duo, password authentication is not available in policy engine; its configuration must be done by another way.
STA offers central policy configuration, requiring fewer clicks and less time to set up various access policies as compared to DUO.
- Limited Reporting**
Do you need to demonstrate compliance to security data privacy standards?
Do you have a large organization or MSP?
How do you plan to administrate users and token lifecycle?

- Duo only offers a Splunk connector so no integration with other SIEM vendors
- No scheduled reports, no custom possible
- Less reports (50+ in STA versus max: 10 in DUO console)
- STA Provide better audit trail for compliance. Prove compliance in a matter of minutes. Uncover anomalies
- Duo has no multi-tier architecture
- STA Allows delegation of administration to local or remote staff: Shared services model enables accounting and inventory management per BU



RSA

	RSA SecurID Access - Competitive Analysis-May 2019	20/01/2020 08:30	Microsoft PowerP...	1,753 KB
	STA vs RSA SecurID Access Battle Card	20/01/2020 08:30	Adobe Acrobat D...	247 KB

BATTLE CARD : SafeNet Trusted Access vs RSA SecurID Access

4 Ways STA is better than RSA

1. Quicker and Easier Set Up
2. Lower Total Cost of Ownership
3. Simpler to manage
4. Stronger reporting

Why Thales?

- IAM Innovator - First vendor to launch cloud MFA service
- 28,000+ IAM customers
- 50+ million end users
- 80% of Fortune 100 companies are our customers

RSA Weaknesses

Weakness	Details
1. Complex set up	Not 100% SaaS Offer Deployment in VPC remains under the responsibility of the customer
2. High TCO	HW token priced on top of user licenses, Active SaaS needed & High set up and maintenance overhead
3. No central console for SSPs	• A console to administrate RSA SecurID Access
4. Poor reporting	• Disparate logging and reporting

Planting Landmines

1. Are you aware that RSA does not offer a full solution focused on a VPC?
2. Are you aware that RSA SecurID Access is complex to deploy?
3. Are you aware of the EXTRA costs & overhead that require RSA SecurID Access?

How do you plan to monitor access and answer to audits?

Avoiding Landmines

RSA is upgrading its customers with SSO capabilities, modern STA and full cloud deployment for free.

RSA has been offering advanced risk-based authentication (RBA) for years! What do you do in terms of advanced analytics?

How many customers do you have? I've never heard of Gemalto.

What is the cost of STA?

OKTA

	Audio Sales elevator pitch OKTA	20/01/2020 08:23	MP3 Format Sound	2,723 KB
	OKTA vs STA features comparison-september 2019	20/01/2020 08:08	Microsoft Word D...	33 KB
	OKTA battle Card Sep 2019	17/01/2020 19:36	Microsoft PowerP...	1,071 KB
	OKTA detailed competitive analysis Sept 2019	20/01/2020 08:09	Microsoft PowerP...	3,143 KB

How are we better than OKTA? The Elevator Pitch

Okta "Workforce Identity" Pricing

STA vs OKTA SSO - Features

STA vs OKTA Adaptive SSO

STA vs OKTA Adaptive MFA/Adaptive SSO

STA can complement OKTA

BATTLE CARD - SafeNet Trusted Access vs Okta

Planting Landmines

Avoiding Landmines



- Tool: Access Management Risk Assessment Tool

- Blog: Access Management from A to Z with Thales and SafeNet Trusted Access

- <https://blog.thalesecurity.com/2020/03/19/enabling-secure-remote-working-in-times-of-crisis-plan-ahead/>



2 Page A4
Jul-19
ELCv7

thalescpl.com

THALES

SafeNet High Speed Encryption Solutions Delivering Data-in-Motion Security without Compromise



Networks are under constant attack and sensitive assets continue to be exposed. More than ever, leveraging encryption is a vital mandate for addressing threats to data as it crosses networks. SafeNet High Speed Encryption solutions from Thales provide customers with a single platform to 'encrypt everywhere'— from network traffic between data centers and the headquarters to backup and disaster recovery sites, whether on premises or in the cloud.

Thales's comprehensive network traffic encryption solutions use Layer 2 and 3 encryption to ensure security without compromise. Ensuring maximum throughput with minimal latency, SafeNet High Speed Encryptors allow customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception—all at an affordable cost and without performance compromise.

SafeNet High Speed Encryption Advantages

Robust Security for Sensitive Traffic

SafeNet High Speed Encryptors, hardware-based, stand-alone appliances deliver robust encryption and FIPS 140-2 Level 3 tamper-resistant key management capabilities. Rigorously tested and certified to be in compliance with the requirements of Common Criteria, the Federal Information Processing Standard (FIPS), the solutions have been vetted by such organizations as the Defense

Information Systems Agency (DISA UC APL) and NATO. SafeNet High Speed Encryption solutions meet the specifications for Suite B cryptographic algorithms (AES-256, ECDSA, ECDH, and SHA-512) for secure communications. Using NIST certified random number generators, SafeNet High Speed Encryptors use high quality keys that are generated and stored in hardware, ensuring that the keys are always under your control, even in multi-tenant environments.

Maximum Performance and High Availability

SafeNet High Speed Encryption solutions have been proven to deliver max uptime in the most demanding, performance intensive environments. The solutions have near-zero latency, and can operate in full-duplex mode at full line speed, without running the risk of packet loss. Further, the small amount of latency is deterministic and is unaffected by packet size. There is also a zero-overhead option available for optimal performance. Plus, these solutions feature descriptive diagnostics that give administrators early warnings of potential issues.

Optimal Flexibility

SafeNet High Speed Encryption solutions offer flexible, vendor-agnostic interoperability, meaning they're compatible with all the leading network vendors throughout your network. They support a wide range of security objectives and network environments, able to adapt to evolving security and network requirements. The product range supports network speeds of 10 Mbps to 100 Gbps,

and platforms range from single to multi-port appliances, and are available in hardware and virtual solutions.

Next Gen High Speed Encryption

Crypto-Agility

SafeNet High Speed Encryptors (HSE) are crypto-agile, meaning they support customizable encryption for a wide range of elliptic and custom curves support. The appliances also allow bring your own entropy capabilities. The crypto-agile platform is future-proof, allowing for responsive deployment of next-gen or custom algorithms. In response to the Quantum threat, SafeNet High Speed Encryptors already leverage Quantum Key Distribution (QKD) and Quantum Random Number Generation (QRNG) capabilities for future-proof data security.

Transport Independent Mode

Transforming the network encryption market, SafeNet High Speed Encryptors are the first to offer Transport Independent Mode (TIM) - network layer independent (Layer 2, Layer 3, and Layer 4*) and protocol agnostic data in motion encryption. By supporting Layer 3, SafeNet High Speed Encryptors offer network operators more configuration options using TCP/IP routing for securing critical data.

SafeNet High Speed Encryptor Family

Thales offers a range of SafeNet High Speed Network Encryptors to ensure the right mix of features and capabilities tailored to your needs and budget. The products in our portfolio are fully interoperable, so a single platform can be used to centrally manage encryptors across single customer links or distributed networks. Each of the encryptors offered can support up to 512 concurrent encrypted connections. Hardware encryptors are certified for FIPS 140-2 Level 3 and Common Criteria EAL+2, EAL4+*.

SafeNet Ethernet Encryptor CN9000 Series

Delivering 100,000,000,000 bits per second of high assurance and secure encrypted data, the CN9000 Series provides mega data security (100 Gbps), with the lowest latency in the industry (<2µs).

SafeNet Ethernet Encryptor CN6000 Series

The CN6000 Series encryptors offer variable-speed licenses from 100 Mbps to 10 Gbps. The CN6140 has a multi-port design that makes this encryptor variable, with speed licenses up to 40 Gbps (4x10 Gbps), highly flexible and cost effective.

SafeNet Ethernet Encryptor CN4000 Series

The CN4000 Encryptors are versatile and compact, offering 10 Mbps-1 Gbps encryption in a small-form factor (SFF) chassis. The CN4000 series is ideal for branch and remote locations, offering cost effective, high-performance encryption, without compromising network performance.

SafeNet Virtual Encryptor CV1000

The CV1000, the first hardened virtual encryptor, is instantly scalable and may be deployed rapidly across hundreds of network links, providing robust encryption protection for data-in-motion. The SafeNet Virtual Encryptor CV1000 is a Virtual Network Function (VNF) that delivers an agile network and reduces capital expenditure requirements. Ideal for organizations that are virtualizing network functions and taking advantage of Software Defined Networking (SDN).



> thalescpl.com <

Announcements - Thales Security Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel: +1 888 744 4776 or +1 954 888 6700 • Fax: +1 954 888 6711 • Email: sales@thalessec.com
 Asia Pacific - Thales Transport & Security (UK) Plc, Unit 4101-3, 41/F, Swire Centre, 240 Queen's Road East, Hong Kong • Tel: +852 2815 9633 • Fax: +852 2815 9741 • Email: asia.pacific@thales-security.com
 Europe, Middle East, Africa - Thales Security, 10000 Boulevard de la Vallée, 92000 Nanterre Cedex, France • Tel: +33 (0)1 41 41 41 41 • Fax: +33 (0)1 41 41 41 41 • Email: europe@thales-security.com

© Thales - July 2019 - ELCv7