KuppingerCole Report

EXECUTIVE VIEW

By John Tolbert

May 21, 2021

Thales SafeNet Trusted Access Platform

Thales is a major player in the global aerospace, defense, and security arena. Thales has a respected line of products and services in cybersecurity and identity protection. Thales SafeNet Trusted Access Platform is a market leading Enterprise Authentication and access management solution. It offers a variety of hard and soft token solutions as well as FIDO compliant authenticators. It is highly scalable and built for environments that require the highest security levels.



By **John Tolbert**

jt@kuppingercole.com

Content

1 Introduction 3

2 Product Description 5

3 Strengths and Challenges 8

4 Related Research 10

Content of Figures 11

Copyright 12

1 Introduction

Organizations around the world have been rapidly modernizing their IAM infrastructures in response to increased cyberattacks and data breaches, enactment of security and privacy regulations, and a shift to remote working. IAM technologies are widely deployed, but can be notoriously difficult to upgrade, which can leave businesses and agencies struggling to meet demands for strong, risk-adaptive yet usable authentication mechanisms. For this reason, IAM customers are turning to modular authentication solutions that can present stronger, contemporary login methods powered by risk engines utilizing Machine Learning (ML) algorithms to detect anomalous behavior and require the collection of additional context information if dictated by security policy to prevent unauthorized access.

Authentication has been one of the areas within IAM that has experienced the most technical advancement. Researchers and vendors have sought to address the inherent weaknesses of password-based authentication and have thus developed many different kinds of authenticators and protocols to increase assurance levels. Biometrics on mobile devices, out-of-band applications, mobile push notifications, and a variety of hardware tokens are noteworthy examples.

Authentication processes have also been improved by behind-the-scenes measures such as the evaluation of user attributes, history, and behavioral analysis; behavioral biometrics; device identity, history, and health; and environmental context, including request types and history, locations, and networks. These unobtrusive means can operate as needed in the background, only interrupting users with explicit need for input when deviations from their established baselines occur, leading to continuous, risk-adaptive authentication.

Regulations written with the goal of improving cybersecurity across various industries have taken effect in multiple jurisdictions. For example, in the US, legislation such as the New York SHIELD Act imposes penalties of up to \$250,000 per incident for organizations that allow unauthorized access to personal information. Whereas the EU's PSD2 requires Strong Customer Authentication for finance customers, NY SHIELD Act will penalize companies that do not adequately protect employees' HR information. Thus, stronger authentication controls for workforce applications are on the radar for many organizations that hold the HR data of New Yorkers.

Access control solutions must balance security and usability. Today's offerings in this area provide multiple authentication mechanisms, including many mobile options and SDKs; risk engines that evaluate numerous definable factors that can be gathered at runtime and compared against enterprise policies; authorization services that can granularly evaluate complex request contexts against pre-defined policies; and out-of-the-box (OOTB) connectors to enable Single Sign-On (SSO) to many popular on-premises and cloud-hosted enterprise applications. Therefore, integration with existing IAM infrastructure should be a primary factor in selecting a suitable product.

Authentication and authorization services are important threads in Identity Fabrics, which are gaining

traction in industry today. An Identity Fabric is an architecture that can be composed of disparate data sources and capabilities delivered as discrete services. Identity Fabrics permit organizations to add and upgrade segments of their infrastructure or contract with service providers to meet business objectives in a more agile manner. Given the widespread availability and adoption of cloud-hosted services running the gamut from IaaS to PaaS to SaaS, more vendors are packaging their solutions in containers such that they can provide the same types of functions regardless of deployment models. This means that on-premises software ships as images or virtual instances that can be deployed on most of the common operating systems or IaaS/PaaS platforms or made available as micro-services via the vendor or MSPs.

The key requirements most organizations look for in access management solutions are:

- Support for multiple authenticator types, such as:
    - Smart Cards, USB tokens, and older form factor hardware tokens
    - Mobile apps and push notifications
    - x.509 certificates
    - Biometrics, especially mobile biometrics leveraging native OS capabilities
    - OTP: HOTP/TOTP over phone, email, and SMS
- Availability of a mobile SDK for customers to write their own secure apps; optional use of Global Platform Secure Element for credential storage and Global Platform Trusted Execution Environment (TEE) for safe mobile app execution
- Adhere to policy-based access control model so that IT departments and Line of Business application owners can define risk-appropriate authentication rules
- Perform run-time risk analysis of behavioral and environmental factors
- Enforce configurable actions including permit, step-up authentication, deny, lock account/device, etc.
- Integrate with other IAM systems to allow SSO, usually via cookie support
- Support identity federation via OAuth2, OIDC, JWT, and SAML
- Integrate with SIEM, SOAR, UBA, and other security systems
- Provide administrators with management dashboards and configurable reporting
- Allow for delegated and role-based administration within the solution
- Process relevant threat intelligence in real-time: using customer's internal, vendor ecosystem collected information, and/or subscriptions to 3rd party services that identify aberrant user behavior, compromised credentials, etc.

2 Product Description

Thales Group is a global leader in the aerospace, defense, and transport industries, headquartered in Paris. SafeNet Trusted Access is a product of their Digital Identity and Security division. This business unit provides identity verification, biometrics, document readers, and credential issuance and management solutions for governments and businesses. Thales is also quite well-known for their encryption solutions. Thales was a pioneer in cloud delivered Identity-as-a-Service (IDaaS). The SafeNet Trusted Access solution can be installed on-premises on Ubuntu and Windows; in IaaS as VMs; and Thales hosts SafeNet Trusted Access as SaaS in their own data centers and in public data centers located in the EU and NA. Licensing is per-user. Licenses include all features of SafeNet Trusted Access: the solution is a fully integrated access management suite that does not require additional fees for advanced functions. Thales has many thousands of SafeNet Trusted Access customers around the world. SafeNet Trusted Access is an Overall and Market Leader in the 2021 edition of KuppingerCole's Leadership Compass on Enterprise Authentication.

CSV and LDAP can be used for bulk provisioning of users. Self-enrollment can be made available, and customer admins can define the related workflows. Email/SMS OTP, help desk, and customized API-driven account recovery mechanisms can be deployed to reduce help desk support costs in cases where credentials need to be recovered quickly.

Thales offers identity proofing services for governments that facilitate the generation of authoritative ID documents such as national ID cards, passports, and drivers' licenses. Thales Identity Verification Suite helps their customers onboard employees, contractors, and consumers with varying degrees of identity assurance as needed by regulation and/or policy. Thales mobile app performs remote registration and document verification by biometric matching (selfie comparison to government-issued credential). Moreover, the biometric analysis utilizes passive liveness detection, which reduces enrollment fraud and improves usability by decreasing the number of clicks and other inconveniences for users at registration time.

SafeNet Trusted Access utilizes its own user database, which is accessible over LDAP and/or SQL through a protected API. Thales provides synchronization kits for Microsoft Active Directory, Azure AD, IBM, Oracle, CA, Okta, and Ping Identity.

SafeNet Trusted Access supports a broad array of authenticators, including Aegis, Authy, Duo, Google, Okta, SAASPASS, and their Thales app-based authenticators; x.509, mobile push notifications, mobile pattern recognition, email/phone/SMS OTP, and Android & iOS biometrics; FIDO 2.0; and CAC/PIV, Feitian, Google Titan, any OATH-based, RSA SecurID, Smart Cards and virtual Smart Cards, Thetis, and Yubikey hardware authenticators. Moreover, their IDPrime 3940, SafeNet eToken, and Thales Multi-App authenticators are FIDO 2 certified. Kerberos, OAuth, OIDC, RADIUS, and SAML protocols are supported for SSO, token exchange, and identity federation. WS-* federation protocols will be supported in the future.

The virtual smart card mechanism allows customers to gain the benefits of strong identity assurance and

authentication without the need for obtaining hardware tokens; rather mobile phones can be used for key and certificate storage.

Thales offers SDKs for customers to build apps that incorporate their mobile authentication capabilities. The SDKs are available for Android, iOS, and Windows 7/10. The SDK can collect some device intelligence attributes, such as device fingerprint, OS version, and jailbreak/root status. Though these parameters can be evaluated by SafeNet, they are not directly exposed for customer application-level processing. SafeNet mobile authenticators do make use of Secure Element on Android and Secure Enclave on iOS for storing certificates and keys securely.

The administrative interface is hierarchical and features drop-down lists that allow customers to create access control policies defining evaluation criteria and any consequent actions. Post-evaluation actions include grant, deny, authenticate once per session, and authenticate upon every access attempt, which enable the creation of step-up authentication flows. Rules within policies can be grouped based on priorities. Policies can include user, group, target application, and context attributes. Security policy authors can construct policies of any depth required, and equivalent actions can be defined such that users can be presented with choices for preferred authentication methods where permissible. Policies cannot be imported as JSON or XACML from other access control systems.

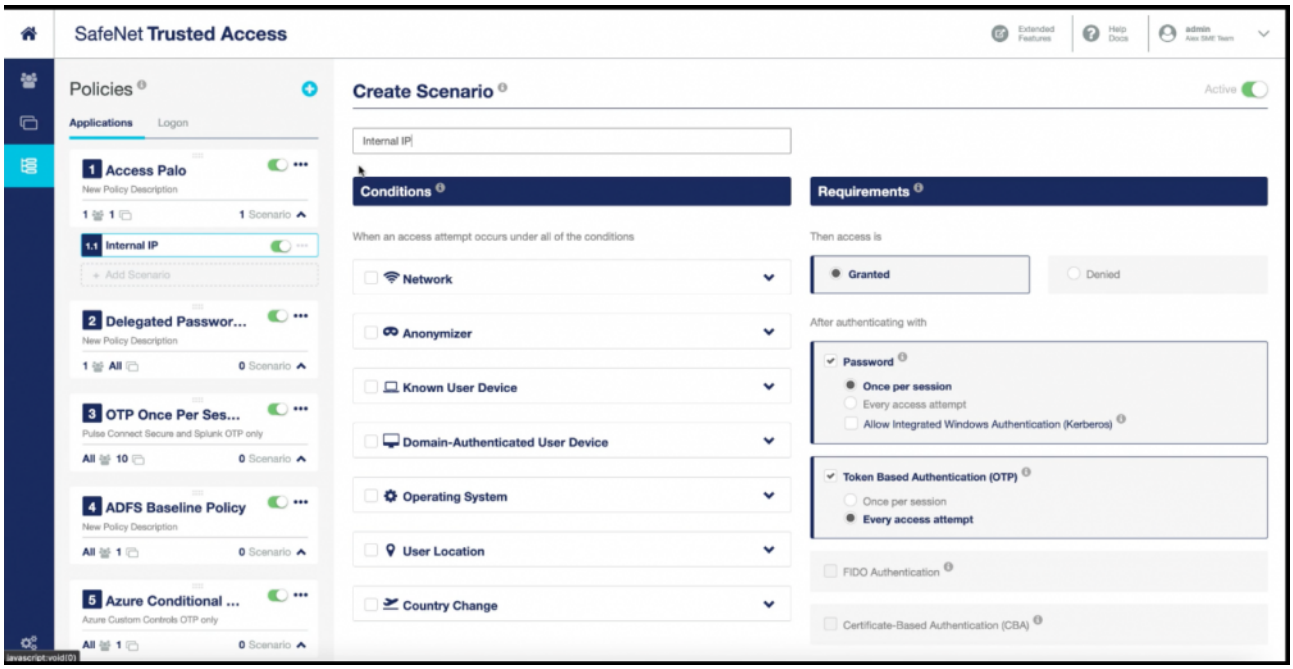


Figure 1: SafeNet Trusted Access Policy Authoring Interface (used with permission from Thales)

Admin console functions can be accessed via REST and SOAP APIs, and JSON and XML formats are supported.

The risk engine can process the following factors: IP address, geo-location, impossible travel, device

fingerprint/ID/type, device health and history, software signatures, and input from user behavioral analysis services. Behavioral biometrics are not currently supported. Due to the service's workforce use case emphasis, compromised credential and fraud reduction intelligence feeds are not processed. Inclusion of cyber threat intelligence as additional risk factors to evaluate is on their roadmap. The risk engine computes event-level scores for internal use only. The risk engine is not exposed via API; thus, it does not interoperate with external authorization systems.

SafeNet Trusted Access can work with a variety of Privileged Access Management (PAM) solutions, including BeyondTrust, CyberArk, Thycotic, and Wallix. For Identity Governance and Administration (IGA), SafeNet can integrate via APIs with Okta, Oracle, Ping Identity, SailPoint, and Saviynt.

SafeNet Trusted Access can serve as the front-end authentication and SSO-enabling service for many popular on-premises and SaaS applications. Examples are shown here, for a complete list see https://cpl.thalesgroup.com/access-management/sta-integrations. For collaboration, SafeNet has federation templates for Atlassian Jira, Box, Cisco WebEx, Dropbox, GitHub Enterprise, GoToMeeting, Hive, Slack, Zoho, and Zoom. For ITSM, templates are available for AlertOps, BMC Remedy, Desk, FreshDesk, FreshService, JitBit, RedHat Ansible, Salesforce, ServiceNow, and Zendesk. For productivity, templates are available for Adobe Creative Cloud, Carbonite, DocuSign, Evernote, G Suite, Microsoft O365, MobileIron, SAP/Concur, Tableau, and Workday. For web and server hosting and development controls, plug-ins are available for Amazon AppStream and AWS, Atlassian BitBucket, Chef Automate, GCP, Jenkins, Oracle Cloud and WebLogic, and SAP Cloud.

SafeNet has agents for some applications that allow interoperability outside of standard API channels. Examples include Microsoft ADFS, Microsoft IIS, Microsoft NPS, Microsoft OWA, Remote Desktop Gateway, Remote Desktop Web, Cisco AnyConnect, Epic Hyperspace, FreeRADIUS, IBM Security Access Manager, Oracle Access Manager, and Oracle Siebel. A reverse-proxy app authentication and authorization is also available to enable IAM integration with other LOB apps that do not adhere to modern or legacy identity concepts and communications.

SafeNet Trusted Access can also provide authentication for the following security consoles: Cisco Meraki, Citrix NetScaler, Palo Alto Cortex XSOAR, SonicWall, Trend Micro, Symantec BlueCoat, and ZScaler.

In addition to many strong MFA methods for SafeNet system administration, the solution also supports fine-grained, role-based, and delegated access control models. SafeNet employs HSM powered data and application layer encryption. Event and incident information can be sent by CEF, JSON, and syslog to SIEMs.

3 Strengths and Challenges

Thales Group is known worldwide for their defense and security work, as evidence by their large customer base for their digital identity and security products and services. Moreover, Thales' SafeNet Trusted Access attests with CSA Star Level 1 for their SaaS offering. Thales was the first company to certify their HSM as US FIPS 140-3 and is FIPS 140-2/CMVP compliant. Thales is also certified on ISO/IEC 9001, 14001, 15408, 27001, and 27018, and SSAE 18 SOC 2 Type 1 & 2. The HSM modules are EAL 4+ and are eIDAS certified for Qualified Signature and Qualified Seal Creation Device.

The broad range of authenticator types supported and the ability to create complex policies means customers can tailor the solution to their requirements, including for the highest levels of identity assurance and security. SafeNet Trusted Access provides granular authorization and access control features and enables SSO to many popular SaaS apps, and has connectors for non-standard and legacy applications as well.

Both the cloud-hosted and on-premises versions can scale to process millions of login events per day. Rapid scaling is achieved by linearly adding instances to either platform type as needed. Thales was one of the first IAM solution providers to enter the IDaaS market, and their modern components are designed to fit alongside existing IAM infrastructure to augment capabilities, rather than requiring customers to effect wholesale migrations. Built-in identity proofing and credential issuance functions facilitate employee, contractor, and customer onboarding.

The addition of flowchart style policy authoring may be perceived as beneficial by some prospective customers. As the IAM market embraces microservice delivered Identity Fabrics, Thales may opt to move in that direction as well. Allowing customer applications, particularly authorization systems, access to the risk engine via APIs or to the output of the risk engine would open SafeNet Trusted Access to opportunities that have such requirements.

Strengths

- IDPrime and SafeNet eTokens are FIDO 2.0 certified
- Good OOTB selection of SSO connectors for a variety of applications, including some uncommon apps
- Support for hard tokens and virtual smart card strong authenticators
- Integrations with most IAM and IDaaS products, meaning SafeNet Trusted Access can co-exist with deployed infrastructure
- Thales Identity Verification for identity proofing and credential issuance
- Strong anti-tampering security mechanisms
- HSM based encryption, with FIPS 140-3 certification
- SOC 2 Type 2, ISO 27001 certifications
- ML anomaly detection models

Challenges

- Risk engine not accessible via API
- No behavioral biometrics
- Additional threat intelligence sources may be beneficial for some customers

4 Related Research

Leadership Compass - Enterprise Authentication Solutions
Leadership Compass - Cloud-based MFA Solutions
Leadership Compass - Adaptive Authentication
Leadership Brief -- Why Adaptive Authentication is a Must

Content of Figures

Figure 1: SafeNet Trusted Access Policy Authoring Interface (used with permission from Thales)

Copyright

©2021 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole´s initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.