MULTI-FACTOR AUTHENTICATION DESIGN AND DEPLOYMENT WITH EIS PLATFORMS

Access Security with Winkk WinkkPass 1.0 and EIS 6.2

WINKK

EIS GROUP®

 mail to: info@winkk.com

Table of Contents

Executive Summary

Comprehensive security requires controlling users' access to sensitive systems, including user authentication. Password-based authentication is vulnerable to a number of direct and secondary attacks. The most common way to mitigate threats of single password authentication in the enterprise is to supplement password authentication with two- and three-factor authentication. The most typical multi-factor authentication (MFA) solution is by supplying a dedicated MFA device to the employees. However, dedicated devices are inflexible, difficult to manage and not feasible for extranet users. In this paper, we describe an MFA solution that eliminates passwords from authentication by using mobile devices and computer vision. Specific architecture integrating Winkk authentication with the EIS® insurance software is documented here.

Introduction

Cyber-Attacks

The information systems industry has seen a rise in cyber-attacks over the past several years, and these attacks continue to grow in volume, complexity, and sophistication. Today's attackers have better resources and are more determined. According to the *Symantec Internet Security Threat Report (1)*, "In 2015, we saw a record-setting total of nine mega-breaches, and the reported number of exposed identities jumped to 429 million". Additionally, the number of spear-phishing incidents has increased 55% since 2015. Security incidents such as these have the potential for lost revenue and liability exposure, as well as the catastrophic impact to a company's brand.

Passwords are the weakest link

Weak password security is a major risk for organizations of all sizes. Based on forensic investigations of prominent breaches, many occurred because attackers were able to guess simple passwords or steal credentials for system access. Targeted phishing attacks are especially damaging when the unauthorized use of administrative passwords allows hackers in the door, enabling them to escalate their system privileges and access sensitive systems, exfiltrate massive amounts of account data, and hide illegal activity. This attack vector allows damages to occur long before victims learn what happened. For example, according to the Verizon 2016 Data Breach Investigations Report (2), 63% of confirmed data breaches were due to weak, unchanged default or stolen passwords. Verizon's forensic analysts note that, "The capture and/or reuse of credentials is used in numerous incident classification patterns. It is used in highly targeted attacks as well as in opportunistic malware infections. It is in the standard toolkit of organized criminal groups and state-affiliated attackers alike."

Multi-factor authentication and compliance

Strong access control has been key part of the enterprise security strategy both for employees and for customers. Multi-factor authentication is not just a strong security practice, but is also mandated by compliance regulations in financial, health and other industries. Regulations requiring MFA include PCIDSS for credit card processing, HIPAA for personally identifiable information and FFIEC for financial institutions.

Audience and purpose

This reference architecture explains a secure multi-factor authentication deployment and operation. It also describes the integration of the EIS® insurance software platform (version 6.2.3) with WinkkPass authentication, which is designed to enforce multi-factor authentication based on the use of mobile devices.

It is tailored to aid security administrators responsible for design, implementation, validation, and utilization of cloud implementations. Hardware configuration, software configuration, and results from the implementation of specific test cases that demonstrate basic operational capabilities are also covered in this document. It is also intended to complement product documentation and is provided as a starting point for the actual development of an authentication solution.

EIS Application Overview

EIS Group empowers Property/Casualty and Group insurers to out-innovate and out-perform their competition with customer-centered, digital-ready core software solutions for rating, underwriting, policy administration, claims, billing, distribution management and customer engagement. In an era of profound industry change and unprecedented competition, EIS Group is enabling carriers around the globe to innovate freely with products and distribution models and successfully engage with today's connected consumer. With EIS software, insurers can free themselves of legacy constraints, drive successful transformation, and build uniquely faster, continuously better, and forever stronger insurance businesses.

EIS Group offers PolicyCore®, an integrated insurance product development and lifecycle management tool; BillingCore® that allows to view account-level and policy-level billing functions, and information enabling customer service staff to resolve billing issues; CustomerCore™ DXP, a digital experience platform for omnichannel interaction and digital solution management for insurers; the EIS Suite® solution, a core administration software solution with components for policy administration, billing, claims, and customer engagement; and ClaimCore®, a P&C claims management solution. EIS Group also offers Pay-As-You-Drive™, a market-ready solution that enables insurers to implement a usage-based auto insurance products; and Software-as-a-Service for insurers. In addition, it offers DistributionCore™ that offers distribution channel and compensation management services; CustomerCore, a customer relationship and communications management solution; Dynamic Analytics that offers business reporting and intelligence services; Product Factory that offers product development and lifecycle management services; and Claim Factory that offers claims workspace configuration solutions. EIS Group was incorporated in 2008 and is based in San Francisco, California with operations in North America, Latin America, Europe, and the Asia Pacific.

Winkk Overview

WinkkPass authentication solution provides organizations with three major benefits. It enables multi-factor authentication with a mobile device; provides centrally managed administration with Microsoft Active Directory; and it eases compliance with a unified audit trail of all authentications across devices, native applications and SaaS services. For deployment, WinkkPass is easy for enterprises and SaaS providers to integrate, typically requiring just a few hours.

WinkkPass uses unique patented optical code technology to establish an out-of-band communication channel for secure authentication. This channel, along with state-of-the-art cryptography and key management creates a mutually authenticated four-way link between any device in need of authentication, the provider, Winkk Cloud Service and the end-users' phone. Effectively, the solution creates an identity vault under the control of the end user, complete with multiple on-line profiles, which can be securely unlocked from the mobile phone. With the WinkkPass mobile app, authentication includes "something you know," "something you have," and "something you are" factors. The result is

very strong protection from hacking, phishing and password re-use, while taking advantage of the bring-your-own-device trend to minimize solution cost and maintenance.

Solution Overview

Adding Winkk multi-factor authentication to the EIS Suite™ solution enables secure access with strong authentication to sensitive client data such as personally identifiable information, insurance policy and other financial data. This integration satisfies the financial industry compliance requirements with ISO 27001 and improves operational security. Winkk integrates with the existing customer Commo Authentication Service (CAS) solutions and does not require changes in existing infrastructure implementation or external hardware tokens to operate. In addition, ability to use employees' own mobile devices without compromising the security enables improved usability and better adoption rates. This model is particularly effective for the franchised / extranet mode of operation embraced by the majority of insurance carriers.

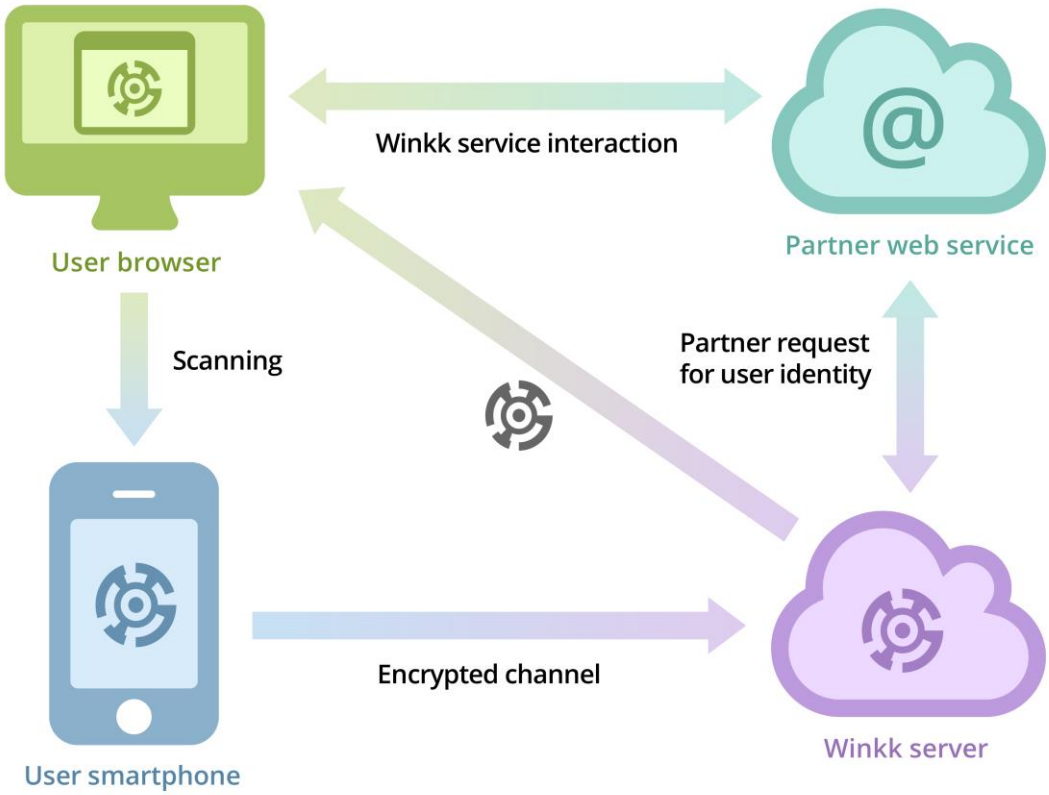
Authentication Workflow

Things to Consider

- Authentication solution should integrate with the existing entitlement systems;
- Authentication solution should work with existing applications deployed in the corporate domain;
- Multi-factor authentication should work for both intranet and extranet users; and
- The solution should be easy to manage.

How it works

WinkkPass™ mobile application, available on iPhone and Android devices, creates a unique cryptographic identity for each of the user's digital profiles.
Each authentication transaction is initiated with the phone scanning a unique dynamic HyperEye™ optical code from the screen of the computer or another device where the application, requiring authentication, will be used.
HyperEye™ is unique patent-pending optical code technology developed by Winkk, which provides faster more reliable recognition than QR and other optical codes.
Initiating authentication is as easy taking a picture of the screen with a phone. When application requests a transaction, a unique code is generated which encodes transaction ID and time limited one-time password. The phone recognizing this dynamic HyperEye™ code represents a one-way out-of-band communication channel which ensures that the application and the phone are mutually authenticated.
When working with SaaS service providers and websites, authentication completes by the application authenticating cryptographically to the in-cloud Winkk service, including transaction and TOTP password information. Once completed, Winkk service sends SAML token to the requesting application via a separate communication channel, secured with a shared secret. This workflow is further illustrated by the diagram below.



When working with enterprise customers, the flow changes to enable individual enterprises to maintain control of their employees identities.

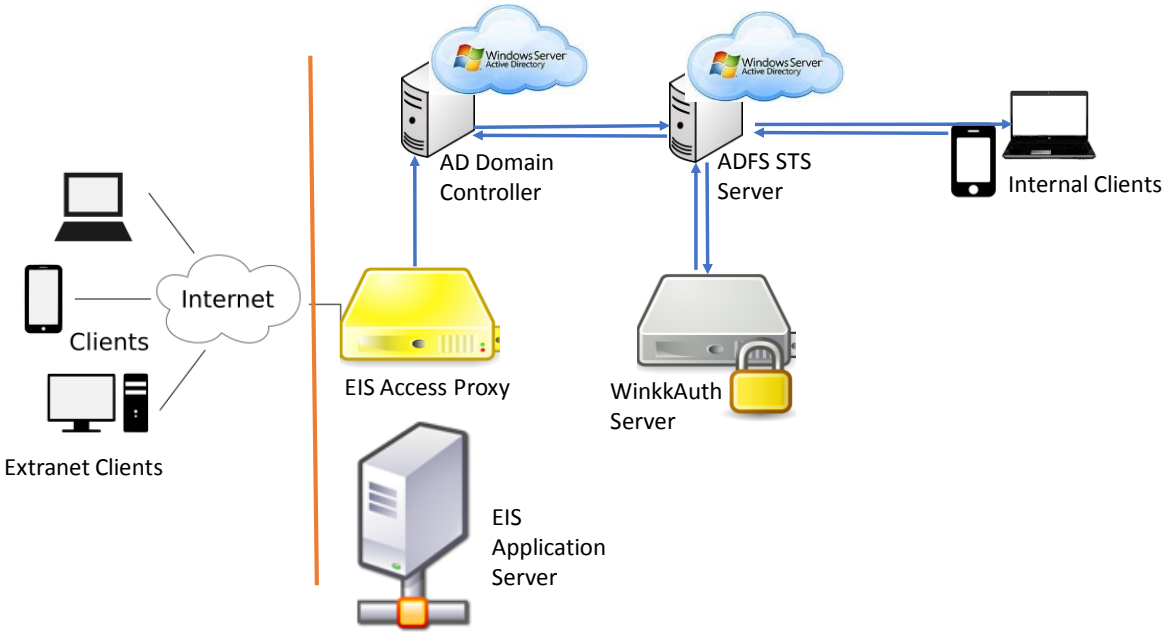
- WinkkAuth endpoint (WA) installs within the enterprise domain perimeter as a docker container or a virtual machine. A special binding is created beween a WinkkPass client profile and employee's domain account.
- Winkk cloud server identifies that the user is an enterprise employee and this profile is controlled by WA and redirects controls. Secondary HyperEye™ code is sent to complete WA authentication.

The rest of the authentication flow is the same as in the case of SaaS providers.

Design Considerations

- Deployment nodes include:
- EIS Application on WebSphere/ CentOS
- EIS Application Proxy
- One or more Microsoft Active Directory Domain Controllers based on Windows 2008 R2 or later
- Microsoft ADFS nstalled on the Domain Controller
- ADFS proxy installedWindows STS server (please note that proxy and STS functions can reside on any DC)
- WinkkAuth server (Separate container)

Architecture Diagram



Installation and Configuration

Winkk Pass Installation and Configuration

The goal is to provide an ability to domain users to authenticate themselves by personal phone without entering their domain credentials at the particular computer.
In this case, domain user authentication is performed via scanning of an optical mark at the computer monitor using Winkk Pass mobile application.
Two main components of the solution are the WinkkAuth server and properly configured Microsoft AD FS / AD FS Proxy.

Preconditions

A company record should be created in the Winkk Pass Partner tool. A secret key will be provided to the company administrator to perform a setup of the WinkkAuth server.

Configuring WinkkAuth server

WinkkAuth server is a dedicated service at the internal network operating under OS Ubuntu. It should be hosted on a separate virtual or physical server in the domain network.
This server is the central part of the Winkk Pass solution. It maintains the database of enrolled domain users, their Kerberos keytabs or NTLM password hashes and a has a connection to the Winkk Pass cloud service.

When requested, it acts on behalf of enrolled domain user. Based on the personal client certificate fingerprint acquired by the Winkk Pass cloud service, WinkkAuth server requests SSO token of particular domain user from AD FS using Kerberos/NTLM domain authentication. Then it transfers the SSO token to the client computer browser.

Addressing

WinkkAuth server should have its own static IP address at the internal domain network. It should have network access to the Winkk Pass cloud service, Web Application server, AD KDC, and internal AD FS STS (connections originated from WinkkAuth server to the Winkk Pass cloud service, Web Application server, AD KDC, and internal AD FS STS should not be blocked).

DMZ and Port Forwarding

Internally, WinkkAuth server listens the following TCP ports to operate:
3611 – HTTPS, a web host to serve client computer browser requests (to show page with optical mark, to set SSO token cookies, to redirect back to domain Web Application).
3613 – HTTPS, the endpoint for Winkk Pass cloud.
As an option, port numbers can be reconfigured as described in the documentation.
For external access, reverse proxy should be configured to direct application URLs with standard ports to the above ports. ADFS proxy described in the diagram above can perform this function or any other existing reverse proxy in the DMZ can be configured for this redirection.

Microsoft Active Directory, AD FS and AD FS Proxy configuration

AD FS and AD FS Proxy need to be configured to forward the authentication requests to the WinkkAuth server for multi-factor authentication.
To provide extra authentication scheme to the domain users, it is needed to add extra special-formed link into the AD FS Sign-In pages. This link will follow domain user to the WinkkAuth server page displaying optical mark to be scanned. WinkkAuth server will also receive target Web Application URL via this link and use it to perform final redirect after SSO token providing to the client computer browser.

Summary and Conclusions

Enterprises looking to increase security, particulary security of acces as well as protection of personally identifiable information as well as to satisfy compliance requirements including ISO 27001 should look at multi-factor authentication, which integrates with existing CAS systems such as Active Directory. The integration presented in this whitepapers enables EIS Suite™ solution to add multi-factor, which allows its insurance and financial industry customers to deploy the EIS Suite™ cloud solution with secure authentication and satisfy the compliance requirements.

Winkk integrates with the existing customer's Common Authentication Service (CAS) solutions and does not require changes in existing infrastructure implementation or external hardware tokens to operate. In addition, ability to use employees' own mobile devices without compromising the security enables improved usability and better adoption rates. This model is particularly effective for the franchised / extranet mode of operation embraced by the majority of insurance carriers.

Endnotes

1. https://www.symantec.com/security-center/threat-report
2. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

About Winkk

Winkk has made passwords obsolete with its unique next-generation WinkkPass authentication solution. It provides multi-factor authentication with mobile devices for easy integration and management by enterprises and SaaS providers, and relieves users of carrying dedicated devices or recalling passwords. Winkk, Inc. is a privately held corporation headquartered in Silicon Valley founded in 2015 by veterans of security and internet companies such as CommerceNet, Intel Corporation, Apple Inc., VMware, Inc., Symantec Corporation and others. Winkk has patents pending on computer vision and cryptographic technologies. For more information, visit winkk.com.