Author Paul Edwards

System Architect,
Tax and Accounting,
Wolters Kluwer (UK) Limited

Wolters Kluwer (UK) Limited

Security White Paper

CCH OneClick

Wolters Kluwer (UK) Limited

Date November 21, 2018
Version 1.1
File CCH OneClick Security White Paper.docx

Version	Date	Author/reviewer	Explanation
1.0	Jan 18	Alex Ayers	Issued
1.1	Nov 20	Paul Edwards / Simon Kershaw	Minor revision

Disclaimer
Wolters Kluwer (UK) Limited has made every effort to ensure the accuracy and completeness of this document. However, Wolters Kluwer (UK) Limited, its staff and agents will not be liable for any errors or omissions and use of the software is subject to the customer's licence with Wolters Kluwer (UK) Limited. This document should not be relied upon as a detailed specification of the system or the software.

Wolters Kluwer (UK) Limited may make changes to this document from time to time.

Copyright

Trademark Rights

Wolters Kluwer (UK) Limited
145 London Road,
Kingston Upon Thames,
Surrey
KT2 6SR

Content

1 Introduction

Helping to protect the confidentiality, integrity and availability of the tools that our customers rely on is a priority for Wolters Kluwer.

This whitepaper gives an overview of how security is built into the CCH OneClick platform and applications.

Securing data and services requires a multi-layered approach covering people, processes and technology. The applications within the CCH OneClick platform have been built from the ground up to be secure, reliable and scalable, using state-of-the-art technologies and running on enterprise-grade infrastructure.

In this whitepaper, we will discuss the technical and organisational controls that we have in place to enable us to provide a secure platform for storing and processing client's data.

2 Secure by Design

2.1 Secure architecture

Several layers of security protect the CCH OneClick platform from external attacks. Only authorised traffic is permitted to connect to CCH OneClick. Multiple firewall layers and technologies are used to block malicious requests from reaching the application. Distributed Denial of Service (DDoS) protection is provided at both the application and platform layer to minimise the impact of an attack on legitimate users of our service.

Network architecture controls include segregation and internal firewalling that permits traffic only between known infrastructure components and is configured to “default deny”. This reduces both the likelihood of occurrence and propagation of a breach at a single network layer.

Our network infrastructure is monitored 24/7 to ensure that we can detect and respond to threats that undermine the availability of the tool and confidentiality of client data.

2.2 Secure applications

Our security teams perform manual and automated security testing against our code and applications to identify potential weaknesses. Output from these activities is reviewed and prioritised for remediation. In addition to internal testing, we have regular penetration testing performed by third-parties and findings are fed into our review and remediation process.

2.3 Data encryption

We use industry-standard HTTPS to protect the confidentiality and integrity of the data passing between user’s browsers, CCH OneClick and any relevant Third-Party services such as HMRC.

Each practice onboarded onto CCH OneClick has its own database which is encrypted, as are all files submitted to CCH OneClick. Passwords are one-way hashed and salted.

2.4 Secure administrator access

A small number of our administration team have access to customer’s data. Access to the production environment is tightly restricted and can only be reached by a secure administration network. Multi-Factor Authentication is enforced for administrators and access is logged and monitored.

3 Secure Culture

3.1 Employee screening

All employees are screened as part of the hiring process. The screening includes rigorous identity checks, verification of previous working history and reference checks.

3.2 Security training

All employees are required to adhere to our Information Security and Data Protection policies which highlight our commitment to keeping customer data secure. Team members involved in the development and support of the CCH OneClick platform and applications undergo additional security training that is targeted to their job roles. For example, architects may receive training in secure design principles while developers focus on secure coding practices and principles.

3.3 Dedicated security teams

Wolters Kluwer have several teams who are dedicated to ensuring the security of our applications and services. Our teams work closely together to provide security leadership, secure design and development, data privacy, security testing, vulnerability management and secure hosting. Our security network spans territories and markets which gives us the ability to rapidly identify and respond to threats across our portfolio of products and services.

4 Secure Operations

4.1 Data Centre Security

CCH OneClick runs on the Microsoft Azure platform and benefit from security, scalability and resilience provided by Azure. The Azure service has achieved several certifications attesting to the management systems and controls that Microsoft have in place to ensure confidentiality, integrity and availability of the platform. These include ISO27001, ISO27018, CSA CCM and SOC 2 Type II.

The Microsoft facilities that host our applications and data operate 24/7 and are designed to be resilient to threats from physical intrusion, power outages and cyber-attack.
More information can be found at the Microsoft Trust Centre: https://www.microsoft.com/en-us/trustcenter

4.2 Monitoring

The CCH OneClick platform and infrastructure is monitored for security events 24/7 by a dedicated team based in the UK. In addition, Microsoft performs 24/7 monitoring across the Azure suite.

4.3 Infrastructure Vulnerability Management

We operate a robust patch management process supported by regular, scheduled vulnerability assessments across the infrastructure hosting our applications.

4.4 Malware Prevention

Malware/virus scanning is performed on all files transferring in and out of the CCH OneClick platform. In addition, the infrastructure hosting our applications is also subject to real-time monitoring for malware.

5 Frequently Asked Questions

Q. Where and how is our data stored?
A. We use Microsoft Azure cloud services to host the CCH OneClick platform. All data is stored in Microsoft UK Data Centres (UK South, UK West). This includes backups and DR.

Q. Is data encrypted in transit and rest?
A. HTTPS is used to provide encrypted communication between customer devices and CCH OneClick. Communications between CCH OneClick and Third Party services, e.g. HMRC, Twinfield, Xero and Sage also use HTTPS to provide security of data in transit.
Encryption at rest is enabled for all Microsoft products that support it. Within CCH OneClick each customer has their own encrypted Azure SQL database. All files sent in messages are encrypted at rest. Open Integration stores data in Azure blob storage which is also encrypted.

Q. What level of encryption is used?
A. HTTPS using TLS uses various cipher suites of either 128 or 256-bit encryption.
Azure SQL databases and Azure blob storage use AES-256 encryption. AES-256 is used to encrypt files stored on our platform.

Q. What cookies are used?
The CCH OneClick platform supports the use of guidance videos and uses an external service from Wistia.

Cookie name	**Type**	**Domain**	**Description**	**Owner**
__distillery	Technical	.accountantspace.co.uk	Used by our video player to remember where you are in a video so that if playback is interrupted (for example, by losing your internet connection) then you can get right back to where you left off.	Our Site
__distillery	Technical	fast.wistia.com	Used by our video player to remember where you are in a video so that if playback is interrupted (for example, by losing your internet connection) then you can get right back to where you left off.	Wistia
.AspNetCore.Client_Portal	Technical	.accountantspace.co.uk	Used as part of the ‘messages and documents’ feature of CCH OneClick to deliver application functionality.	Our Site
.AspNetCore.Cookies	Technical	.accountantspace.co.uk	Used as part of the ‘making tax digital’ feature to deliver application functionality.	Our Site
access-token	Technical	.accountantspace.co.uk	Used as part of the ‘open integration’ feature to deliver application functionality.	Our Site
Ai_session	Technical	.accountantspace.co.uk	Used to facilitate error logging	Our Site
Ai_user	Technical	.accountantspace.co.uk	Used to facilitate error logging	Our Site
Incap_ses_*	Technical	.accountantspace.co.uk	Used by network security devices	Our Site

Visid_incap_*	Technical	.accountantspace.co.uk	Used by network security devices	Our Site

To support the operation of the service, various settings are held in session storage in the user's browser and are cleared when the browser session is terminated.

Q. Who can access customer data?
A. Customers control who in their organisation can access the data in the CCH OneClick platform. CCH OneClick applications respect restrictions applied within CCH Central e.g. Client List.
A small number of our administration team can access the data held in customer databases. Access to the production databases is tightly restricted and can only be accessed via a secure administration network. Strong authentication controls are in place to secure access to the administration network and access is logged and monitored.

Q. Who owns the data?
A. Data that's not anonymised such as financial data used for compliance purposes is owned by the customer.
As we build out our vision Wolters Kluwer is looking at aggregating data which will support activities such as Business Intelligence, Reporting and Benchmarking and to support this the data would be anonymised and owned by Wolters Kluwer.

Q. Who is responsible for the data?
A. Trust in cloud computing is based on the principle of shared responsibility. Wolters Kluwer is responsible for providing a secure platform for data storage and processing. Customers are responsible for operating controls to ensure that the data they put on the platform is accurate and only processed by appropriately authorised individuals.

Q: What can the data be used for by Wolters Kluwer?
A. The initial focus of the Open Integration Programme is to access and use financial data from bookkeeping systems to support compliance processes such as Accounts Production and Making Tax Digital. The Open Integration Programme ensures data is collected from 3rd party systems and then made available, removing the necessity for training on multiple bookkeeping solutions.
Our vision with the Open Integration Programme is to be able to make greater use of this data enabling the practitioner to gain added value through benchmarking, data analysis and pro-active reporting. This anonymised data will provide practitioners with the information they need to deliver pro-active advisory services. To fulfil this vision there is additional work Wolters Kluwer will be focusing on in the next year.

Q. Is data anonymised and to what extent?
A. Currently data is not anonymised as it is remains under the control and ownership of our customers.
As we build out our vision Wolters Kluwer is looking at aggregating data which will support activities such as Business Intelligence, Reporting and Benchmarking and to support this the data would be anonymised and owned by Wolters Kluwer.

Q. Can practices or customers opt to be excluded from external data use by WK?
A. Yes, the Open Integration Programme is an optional feature that can be used by clients and if switched off and not configured there is no connection.

Q. What security testing is performed?
A. We put our applications through a rigorous testing process which includes static and dynamic application security testing (SAST, DAST); monthly vulnerability assessments; internal and Third Party penetration testing. In addition, the infrastructure that we host on is subject to regular vulnerability assessments and annual penetration testing.

Q. What frequency is infrastructure patched?
A. Infrastructure is patched weekly.

Q. What frequency are applications patched?
A. Application patching is aligned with our published maintenance schedule. Any significant security issues that we identify are dealt with under our emergency fix process and follow our standard out-of-schedule notification process.

Q. What control do customers have over security?
A. User lifecycle management is performed via CCH Central. Permissions applied in CCH Central e.g. Client List restrictions are applied in CCH OneClick. As we develop the range of applications on CCH OneClick, we will be extending the data security and task permissions concept to ensure new functionality can be appropriately restricted.

6 Practice Mobile

Our Practice Mobile app works across phone platforms to enable teams to securely communicate with clients when out of the office.

Recognising the risks associated with mobile devices, we have built in several controls to ensure that communications remain confidential.

6.1 Authentication and Authorisation

Practice Mobile users log in with the credentials they use for CCH OneClick. Once logged into the app, users are only able to see the messages that they are authorised for.

To reduce the risk of data loss in the event of a lost device, the application has a time-out that requires users to re-enter their password after a period of inactivity. This is independent of any lock settings on the mobile device.

6.2 Encryption

All communications between the Practice Mobile app, CCH Central and CCH OneClick are encrypted using HTTPS. All documents stored on CCH OneClick are encrypted at rest. All documents stored on CCH OneClick are scanned for malware before they are encrypted and saved.

6.3 Shared Responsibility

The security of mobile apps is a shared responsibility. Practices and clients have a role to play in ensuring that data on mobile devices remains secure. There are several practical steps that can be taken to reduce the likelihood of sensitive data falling into the wrong hands.

1. Activate a lock screen and enforce a timeout after a period of inactivity. There are many options including PIN, passcode and, if supported by the device, biometric locks.
2. Encrypt the device. iOS devices running version 8 or above do this as standard when a lock screen is set with a strong passcode. Device encryption is supported as standard on devices running Android and Windows.
3. Only use apps from official app stores. This doesn't completely remove the risk that a device will be infected by malware which may compromise the data on your device, it will significantly reduce it.
4. Enable remote wipes for devices holding sensitive data. This is supported as standard on devices running iOS, Android and Windows.