SMART-DI
Group

Documento Técnico

Servicios en la Nube de Smart-di

Aviso Legal

Los servicios mencionados en este documento contienen información que es propiedad de Smart-DI Group Inc. Es importante tener en cuenta que estos servicios están en constante desarrollo y evolución, por lo que la información aquí proporcionada está sujeta a cambios sin previo aviso. Los derechos de propiedad intelectual e información contenidos en este documento son confidenciales y exclusivos de Smart-DI Group, y solo pueden ser accedidos por esta organización y el cliente. Si encuentra algún error en la documentación, le pedimos que nos lo comunique por escrito al siguiente correo electrónico: admin@smart-di.com.

Smart-DI no puede garantizar que este documento esté libre de errores.

Queda estrictamente prohibida cualquier reproducción total o parcial de esta publicación por cualquier medio (electrónico, mecánico, fotocopia, grabación u otros), así como su almacenamiento en un sistema de recuperación de datos o su transmisión, sin el previo consentimiento por escrito de Smart-DI Group.

Renuncia de Responsabilidad

Este documento ha sido redactado con cuidado y la información incluida proviene de fuentes confiables. Sin embargo, no asumimos ninguna responsabilidad por la precisión, integridad o pertinencia de la información proporcionada. Por lo tanto, no se aceptarán reclamaciones derivadas del uso de la información contenida en este documento. Smart-DI Group se reserva el derecho de modificar esta información en cualquier momento sin previo aviso. Además, recomendamos encarecidamente a los usuarios que verifiquen la información actualizada y consulten a profesionales cualificados antes de tomar decisiones basadas en la misma. Esta renuncia de responsabilidad se aplica tanto a Smart-DI Group como a sus empleados, directores, afiliados y socios comerciales.

Finalidad de este documento

Insight PRINT es una solución cuya finalidad es realizar el análisis de información de impresión generada por soluciones DAS – Document Accounting Solutions (MyQ, Equitrac, PaperCut, Docupro, OneQ, etc.), soluciones MPS – Managed Print Services y otras. Smartker es un servicio de gestión documental y automatización de flujos de trabajo. CaptureAI es una solución de captura y digitalización de información. Estas tres soluciones/servicios conforman actualmente la plataforma de servicios de Smart-DI, llamada Smart-DI Services.

El presente documento describe las características técnicas de la plataforma Smart-DI Services, centrándose en las medidas técnicas y de proceso que Smart-DI Group ha implementado en las áreas de seguridad (seguridad TI y protección de datos) y capacidad de ampliación de la plataforma.

Este documento está dirigido, en concreto, a empleados técnicos de posibles clientes, empresas interesadas y socios de ventas, así como a consultores o medios especializados.

Finalidad de este documento (detallada):

El propósito de este documento es describir las características técnicas de la plataforma Smart-DI Services, que incluye servicios como Insight PRINT, Smartker y CaptureAI. Estas soluciones fueron diseñadas, entre otras cosas, para realizar el análisis de información de impresión generada por soluciones DAS (Document Accounting Solutions) como MyQ, Equitrac, PaperCut, Docupro, OneQ, etc.; soluciones MPS (Managed Print Services) como NDD MPS, Nubeprint, KFS (Kyocera Fleet Services); y soluciones IMS (Incident Management Solutions). Además, ofrecen servicios de gestión documental y automatización de flujos de trabajo a través de Smartker, y proporcionan una solución de captura y digitalización de información mediante CaptureAI. Estos son algunos de los servicios que conforman la plataforma integral de Smart-DI Services.

El enfoque principal de este documento se centra en las medidas técnicas y procesos implementados por Smart-DI Group en las áreas de seguridad (seguridad TI y protección de datos) y capacidad de expansión de la plataforma.

Este documento está dirigido específicamente a empleados técnicos de posibles clientes, empresas interesadas y socios de ventas, así como a consultores y medios especializados que deseen obtener información detallada sobre la plataforma Smart-DI Services.

Introducción

Smart-DI Services ofrece un conjunto de soluciones o servicios basados en el modelo "Software as a Service" (SaaS), los cuales se prestan en un entorno compartido para múltiples clientes y usuarios. Para ofrecer estos servicios, Smart-DI Services utiliza servicios especializados de terceros, como AWS, Microsoft Azure y IONOS. Todos los documentos y archivos del cliente que requieran ser almacenados en Smartker se guardarán exclusivamente utilizando el servicio de Azure Storage.

No se almacenará ningún documento o archivo en unidades locales.

Según el tamaño y los requisitos del cliente, la información de todos los servicios se almacena en una base de datos relacional PostgreSQL. Por defecto, esta base de datos se aloja en nuestra infraestructura de servidores de IONOS. Sin embargo, según los requisitos del cliente, también se puede alojar en Azure Database for PostgreSQL o utilizar la infraestructura en la nube del propio cliente. Ambos servicios cuentan con procedimientos de copia de seguridad diaria a nivel de cada base de datos y de cada instancia. Además, se siguen las mejores prácticas de seguridad de la información, las cuales permiten recuperar la información en el menor tiempo posible en caso de presentarse alguna incidencia de "desastre" del servicio.

Este documento se limita a describir los servicios ofrecidos y desarrollados directamente por Smart-DI. Nuestros asociados comerciales (AWS, Microsoft Azure y IONOS) proporcionan información detallada sobre el funcionamiento de los servicios que incorporamos de ellos, como Microsoft Azure Storage, Microsoft Azure Database for PostgreSQL, Lambdas AWS, Airflow AWS, Microsoft PowerBI, Microsoft Azure Defender, Microsoft Authentication Services, etc. Asimismo, estos asociados describen las medidas relacionadas con la seguridad TI y la protección de datos en las que se basa Smart-DI.

Seguridad

Los datos del cliente utilizados en las plataformas de Smart-DI Services están protegidos de acuerdo con las normas de tecnología generalmente aceptadas (GDPR, ISO 27001, etc.). Esto se logra mediante el uso de la infraestructura de TI de IONOS Hosting Services y las tecnologías de Microsoft Azure AD Authentication Services, Microsoft Azure Storage Services y Microsoft Azure Database for PostgreSQL, asegurándose de que se cumplan las directivas actuales de protección de datos.

Para la codificación del tráfico de datos entre los usuarios y el centro de datos, se utiliza el protocolo TLS (Secure Transport Layer), sucesor del SSL. TLS se emplea para todo el tráfico basado en HTTP (HTTPS) y TCP, y los usuarios pueden verificar en su navegador si su conexión está segura y validada.

En cuanto a los servicios de recolección de información de Insight PRINT, se utiliza un servicio de conexión directa a nuestra plataforma, donde la información se envía cifrada de punta a punta al centro de datos de Smart-DI.

Codificación de documentos:

Todos los documentos archivados en la plataforma Smart-DI Services se encriptan automáticamente utilizando el método AES (Advanced Encryption Standard) de 256 bits, que es un método criptográfico simétrico de alta seguridad. Esta codificación AES genera un par de claves asimétricas para cada archivo, donde la clave privada se utiliza para codificar las claves simétricas generadas durante la codificación de los documentos. A su vez, la clave de codificación del archivo se vuelve a codificar con una clave maestra.

Para lograr la máxima protección, Smart-DI Services utiliza una longitud de codificación de 256 bits con AES, lo que impide la detección de patrones y hace que las claves de codificación sean imposibles de calcular incluso mediante criptoanálisis.

Los datos del cliente utilizados y almacenados en la plataforma de Smart-DI Services están protegidos de acuerdo con las mejores prácticas de seguridad reconocidas en la industria. Para lograr esto, nos apoyamos en la infraestructura de TI de IONOS Hosting Services y en las tecnologías proporcionadas por Microsoft Azure, como Microsoft Azure AD Authentication Services, Microsoft Azure Storage Services, Microsoft Azure Database for PostgreSQL, etc. Estas tecnologías nos permiten cumplir con las directivas actuales de protección de datos, incluyendo normas como el Reglamento General de Protección de Datos (GDPR) y las pautas de la norma ISO 27001, entre otras. Además, todos nuestros servicios están protegidos por un **Web Application Firewall (WAF) de Cloudflare,** que minimiza riesgos de seguridad y permite proporcionar esquemas de seguridad adicionales personalizados para cada cliente.

Seguridad de TI:

Smart-DI se esfuerza por garantizar la seguridad de los datos mediante la implementación de medidas de protección. Estas incluyen la encriptación de documentos, bases de datos y comunicaciones, así como un sofisticado concepto de derechos y/o restricciones de acceso a la información y auditorías de seguridad. Smart-DI Group está comprometida a seguir las mejores prácticas de seguridad y a actualizar constantemente nuestros sistemas para proteger los datos de nuestros clientes y minimizar cualquier riesgo.

En cuanto a la comunicación, en el centro de datos de IONOS utilizado por Smart-DI, todos los datos de comunicación del cliente están protegidos mediante una VPN (Red Privada Virtual). Además, la infraestructura de red está virtualizada y la red virtual está protegida contra amenazas externas.

Concepto de derechos de acceso y restricción a los documentos:

Las soluciones de Smart-DI Services utilizan un sofisticado sistema de derechos de acceso, que puede diferenciar entre derechos funcionales y derechos de acceso en los servicios proporcionados a través de la plataforma Smart-DI Services (Insight PRINT, Smartker y CaptureAI).

Los derechos funcionales se asignan por organización de Smart-DI y se refieren a las acciones que un usuario puede realizar dentro de cada solución. Estas acciones pueden incluir la administración de usuarios, la configuración de archivos y bandejas, el diseño de flujos de trabajo, el uso de sellos, la administración de departamentos, indicadores, paneles de control, entre otros.

Los derechos de acceso se refieren al acceso a información, carpetas específicas y a los documentos almacenados en ellas. Estos derechos pueden incluir la gestión de autorizaciones administrativas, como derechos de diálogo o descarga de documentos, la búsqueda, edición o eliminación de autorizaciones generales para documentos en un archivo, y autorizaciones de superposición, como la aplicación de sellos, anotaciones y elementos gráficos a los documentos, o la eliminación de anotaciones. También se pueden asignar autorizaciones para campos de índice, como cambiar los contenidos de los campos o utilizar entradas de campos que no están en una lista de selección.

Derechos para usuarios y administradores:

En todas las configuraciones de Smart-DI Services, como bandejas, archivos o formularios, se asignan permisos tanto a los usuarios directamente como a través de roles. Existen dos tipos diferentes de permisos: los derechos de usuario permiten el uso del objeto en cuestión, mientras que los derechos de administrador permiten realizar cambios en el objeto o su configuración.

Restricción de acceso mediante separación de datos:

Las soluciones de Smart-DI Services separan de manera estricta los datos del cliente de los datos del sistema. Esto significa que la plataforma utiliza una organización (base de datos, usuarios, accesos, roles, etc.) de los servicios de Smart-DI para cada cliente. Esto permite que los servicios de Smart-DI utilicen nuestros propios recursos de infraestructura o los recursos del cliente, según sea necesario. Por ejemplo, los servicios pueden utilizar la base de datos y las cuentas de Azure Storage del cliente.

Auditoría de seguridad:

Se realizan pruebas regulares de penetración externa e interna para mantener la seguridad de los sistemas. Los auditores externos examinan cuidadosamente los resultados de estas pruebas, que se llevan a cabo mensualmente o antes de incorporar una nueva funcionalidad a la plataforma.

Además, Azure Security Services proporciona informes detallados sobre los riesgos identificados para que cualquier problema que surja con los servicios en Microsoft Azure pueda ser resuelto rápidamente.

Los clientes tienen la capacidad de registrar y exportar los registros de documentos, archivos y organizaciones dentro de su propia organización en formato CSV universal para facilitar su lectura. Estos registros permiten, por ejemplo, rastrear quién modificó una determinada configuración o guardó/eliminó documentos. Los registros también demuestran el cumplimiento de las directrices legales.

Análisis de datos telemétricos:

En los análisis de seguridad en tiempo real de los datos telemétricos, se comprueba si se producen eventos inusuales dentro de los sistemas de Smart-DI en comparación con el servicio normal. En caso de detección de tales eventos, se tomarán las medidas adecuadas. Las investigaciones incluyen:

- Acceso a la base de datos (acceso y semántica de comandos).
- Índice de errores.
- Modificaciones en el rendimiento.
- Intentos de conexión.
- Actualizaciones críticas del sistema.
- Tráfico de red.

Seguridad y protección de datos

Smart-DI Services garantiza la seguridad, protección y recuperación de los datos del cliente de forma fiable cuando se configura y maneja adecuadamente. Por lo tanto, brinda apoyo al cliente en su cumplimiento con la ley de protección de datos regional.

Seguridad de los datos en el servicio Smartker:

Todos los documentos utilizados por los clientes (datos productivos) se almacenan en un centro de datos de Microsoft Azure (ubicación principal US-EAST). Esto se aplica tanto a los documentos en archivos como a los de las bandejas. Además, en caso de ser requerido por el cliente (con un costo adicional) y a fin de salvaguardar todo el inventario de datos productivos para grandes datos, como terremotos o accidentes aéreos, se podrían realizar copias de cada documento en un segundo centro de datos ubicado en otra región, US-CENTRAL.

Protección de datos:

El funcionamiento de los sistemas está sujeto a la ley regional de protección de datos. Los datos de nuestros clientes de la región de América del Norte y América del Sur se alojan en centros de datos ubicados en Estados Unidos. La ubicación principal actual se encuentra en el estado de Nueva York y la alterna en Texas. Los datos de clientes americanos están sujetos a la política de protección de datos de EE. UU.

Copia de seguridad Smartker y CaptureAI:

Si el cliente ha contratado el servicio adicional de almacenamiento de copias en un centro de datos secundario y por error alguno de los usuarios eliminó documentos requeridos, es posible restaurarlos en caso necesario. Incluso si los documentos se han modificado incorrectamente, se puede restaurar cualquier borrador anterior.

En ambos casos, se aplican las siguientes restricciones:

Para permitir un restablecimiento, tanto las bases de datos como los documentos están respaldados por Smart-DI como copias de seguridad en su propio Cold Storage. Dicho Cold Storage se encuentra en un centro de datos de Microsoft en el estado de Texas (EE. UU.).
Para ello, se realiza y se almacena una copia de seguridad de cada documento. Dicha copia se realiza poco después de que el documento se haya guardado o modificado en Smartker. En el caso de una copia de seguridad tras la modificación del documento, se crea una nueva copia del documento. Dicha copia se guarda, además de las copias de seguridad existentes del documento. Esto siempre se aplica, tanto con la versión de documentos activada como no activada en Smartker.

Al importar manualmente los datos de la copia de seguridad en el sistema productivo, una organización de Smart-DI Services se puede restaurar completamente en cooperación con nuestro grupo de soporte. Si el cliente requiere datos de la copia de seguridad debido a un manejo inadecuado (por ejemplo, eliminación o modificación accidental de documentos), el cliente se hará cargo de los gastos de soporte en la recuperación.

Además de los documentos, las copias de seguridad completas de las bases de datos de PostgreSQL se llevan a cabo en Cold Storage, principalmente los fines de semana y en horario nocturno en la región.

Copia de seguridad Insight PRINT:

Para permitir un restablecimiento de las bases de datos y del servicio completo de Insight PRINT, cada base de datos de los clientes es respaldada de forma diaria y almacenada en un Datacenter de Microsoft en el Este de EE. UU. (Nueva York). Adicionalmente, se hace una copia de seguridad de la imagen de los servidores de bases de datos de forma diaria y se almacena en un centro de datos alterno ubicado en el estado de Texas (EE. UU.)

Capacidad y rendimiento

Smart-DI Services Capacidad de ampliación:

Tanto Smart-DI como Azure ID Services, Amazon Web Services, Azure Storage y IONOS Hosting Services ofrecen métodos y tecnologías de capacidad de ampliación extensiva de la infraestructura en caso de ser requeridos, los cuales son utilizados por los servicios de Smart-DI Services.

Capacidad de ampliación por cliente:

Los servicios ofrecidos son compatibles con todo tipo y tamaño de empresas. Se pueden adaptar de manera flexible en términos de volumen de almacenamiento, capacidad de procesamiento y número de licencias de usuario al tamaño de la empresa en cuestión y al volumen de datos y/o documentos procesados.

Capacidad de ampliación del sistema Smart-DI Services:

La plataforma de Smart-DI Services tiene la capacidad de ampliarse automáticamente según la cantidad de usuarios, la cantidad de datos y el tamaño de la carga de procesamiento. Dado que Smart-DI Services es una Public Cloud, la ampliación se realiza por sistema y no por organización del cliente. Actualmente, la configuración mínima de los servidores que se usan para la administración de los diferentes servicios es de mínimo 12 Cores, 64 GB de RAM y Discos Duros SSD/NVMe; sin embargo, se debe tener en cuenta que la configuración es “elástica” y puede cambiar automáticamente de acuerdo a lo mencionado anteriormente.

Rendimiento y distribución de carga:

La distribución de la carga en todos los servicios disponibles garantiza un alto rendimiento constante de todos los servicios disponibles en la plataforma de Smart-DI Services, respondiendo rápida y dinámicamente a condiciones de carga fluctuantes a través de una escala mayor o menor de los servicios existentes o la agregación de servicios completos.

Capacidad de integración:

Para maximizar el uso de la administración del control de impresión, la gestión de documentos y la automatización del flujo de trabajo, la plataforma de Smart-DI Services se podría conectar a prácticamente cualquier aplicación empresarial. Esto funciona solamente si dicha aplicación funciona como un sistema basado en la nube y requiere ser coordinada a través de nuestro grupo de ingenieros de servicios profesionales.

Control y mantenimiento

El centro de datos de IONOS y los servicios de monitoreo de Microsoft Azure controlan constantemente todas las operaciones efectuadas dentro de la plataforma de Smart-DI. Los incidentes destacados se notifican automáticamente a nuestro grupo de soporte para su valoración y revisión. El control incluye:

- Controles constantes del rendimiento.

- Pruebas completas de las funciones básicas de los servicios de Smart-DI.

- Revisión de patrones de uso de clientes, como el tiempo que acceden a los servicios, el número de usuarios durante el día, la cantidad de acciones que realizan los clientes en una ventana de tiempo determinada (por ejemplo, la búsqueda y archivado de documentos, inicio de sesión) para permitir mejoras de rendimiento.

En el caso de irregularidades, el soporte del sistema de Smart-DI Services interviene inmediatamente con servicio ininterrumpido.

Revisiones y actualización:

Al menos 2 veces al año, está planeado el lanzamiento de una nueva versión de los servicios de Smart-DI y esta nueva versión debe publicarse para ser usada por todos los clientes/organizaciones. Para ello, la organización se desconecta por un tiempo máximo de 8 horas, se realiza la actualización y, a continuación, la organización vuelve a conectarse con la nueva versión de los servicios de Smart-DI.

Smart-DI Group informa a los clientes sobre la actualización planificada con cuatro semanas de antelación. En caso de error, la organización se volverá a poner en línea con la versión anterior, para evitar períodos de inactividad prolongados.

Los componentes instalados localmente (Desktop Apps como Insight PRINT Client, Smartker Connector, Smart-DI Plugins, etc.) siempre deben mantener a los clientes actualizados. Los propios usuarios pueden realizar dichas actualizaciones de forma sencilla, siempre y cuando estén autorizados para instalar software localmente. De lo contrario, el administrador de TI puede realizar la actualización con la ayuda de nuestro grupo de soporte de aplicaciones.

Mantenimiento:

Ciertas actividades de mantenimiento requieren derechos de administración completos o avanzados a los sistemas Smart-DI Services. Para garantizar la seguridad de los datos que cumple con las normas de tecnología generalmente aceptadas, el acceso de los administradores de mantenimiento está sujeto a registro y puede ser visualizado y monitoreado por el cliente.

Además, se aplican los siguientes mecanismos de seguridad:

- Todos los accesos a los sistemas de Smart-DI Services se realizan a través de una sesión RDP con puertos y usuarios controlados.

- Para poder iniciar una sesión RDP, un administrador debe seleccionarla a través de direcciones IP definidas por el Firewall Externo y especialmente protegidas en una VPN que está protegida por certificados y solo está disponible para los administradores.

- Cada administrador de Smart-DI Services cuenta con su propia identificación. Por lo tanto, siempre se puede saber quién ha iniciado sesión en qué sistema.

- Todos los administradores están capacitados y han recibido formación específica sobre la manipulación y protección de datos, como certificados y contraseñas.

Finalización del contrato

Transferencia de datos al final del contrato:

Los datos del cliente son siempre propiedad del cliente. En caso de que un cliente decida rescindir el contrato, Smart-DI le brindará asistencia para descargar toda la información almacenada en las bases de datos o de los documentos de Smartker. Existen dos opciones para esto:

- En Smartker, las pequeñas cantidades de documentos pueden exportarse de una manera fácil y rápida usando la funcionalidad de Folder Export, la cual le permitirá almacenar todos los documentos conservando la estructura del gestor de documentos.

Esta opción está limitada a un máximo de 30,000 documentos o 10 GB de almacenamiento. En caso de tener cantidades mayores de documentos, se debe coordinar con nuestro grupo de soporte para realizar el proceso de exportación de manera desatendida.

- Los especialistas de Smart-DI Professional Services prestan ayuda en caso de grandes volúmenes de datos y muchos documentos integrados en los procesos actuales. Sus servicios de pago ofrecen las siguientes ventajas:

- Tras consultar con el cliente, el acceso a los documentos se realiza directamente en el centro de datos y, por lo tanto, se transfieren grandes cantidades de datos en el menor tiempo posible.

- Los documentos dinámicos e integrados en los procesos actuales se migran a los procesos de un nuevo sistema de manera oportuna, minimizando así las interrupciones de los flujos de trabajo.

- Se desarrollan soluciones a medida del flujo de trabajo y los tipos de documentos utilizados por los clientes.

- Insight PRINT: La descarga de las bases de datos de la información almacenada en Insight PRINT se refiere a todos los datos “crudos” (información proveniente de los sistemas externos) extraídos de las herramientas de control de impresión, de MPS, etc. No se refiere al modelo de business intelligence generado con esos datos, que es propiedad intelectual de Smart-DI.

Tras la rescisión del contrato, todos los datos del cliente dentro de los sistemas de Smart-DI Services y todos los datos de las copias de seguridad se eliminarán de manera segura e irrevocable: después de 30 días en la ubicación principal y durante el siguiente trimestre, en Cold Storage. A partir de este momento, la recuperación de datos ya no será posible.

Cumplimiento y legalidad

Microsoft y Amazon Web Services se han destacado en el sector por el establecimiento de requisitos claros de seguridad y privacidad, y por cumplir estos requisitos de forma constante. Ambos cumplen un amplio abanico de normas internacionales y específicas del sector, como el Reglamento General de Protección de Datos (RGPD), ISO 27001, HIPAA, FedRAMP, SOC 1 y SOC 2.

Auditorías de terceros rigurosas, como las del Instituto Británico de Normalización, confirman que Azure se adhiere a los estrictos controles de seguridad que estos estándares exigen. Más información sobre las certificaciones de Microsoft Azure.

Modificaciones a este documento sobre Smart-DI Services

Smart-DI se reserva el derecho a modificar el contenido de este White Paper por razones legítimas, en particular con respecto a los servicios y estándares descritos, ya sea por la introducción de nuevos servicios o estándares, modificaciones en la oferta de servicios de los proveedores de servicios utilizados (en particular, Microsoft) o prescripciones legales u oficiales modificadas.