MindView Drive Technische Spezifikation

Dokumentrevision: 2.10

MatchWare Inc.
511 West Bay Street
Suite 480
Tampa, FL 33606
United States

T: +1-813-254-6644
usa@matchware.com

MatchWare Ltd
3-5 Red Lion Street
Richmond, TW9 1RJ, UK
United Kingdom

T: +44 (0)20 8940 9700
london@matchware.com

MatchWare France
38 rue Servan
75544 Paris Cedex 11
France

T: +33 (0)810 000 172
vente@matchware.com

MatchWare GmbH
Anckelmannsplatz 1
20537 Hamburg
Deutschland

T: +49 (0) 40 543764
hamburg@matchware.com

MatchWare A/S
Thomas Koppels Gade 30
DK-8000, Aarhus C
Denmark

T: +45 86 20 88 20
aarhus@matchware.com

MatchWare
Software for Creative Minds

Inhalt

MindView Drive 1
Überblick 3
Kundendaten 3
Speicherort 3
Online-Dokumentenspeicherung im Ruhezustand 5
Cloud-Dienste 6
Arbeitsinstanzen 6
Datenfluss bei Online-Dokumenten 7
Systemdaten im Transit 8
E-Mails 9
Sicherung und Aufbewahrung 9
Autorisierung 9
MatchWare Anmeldung 9
Zwei-Faktor-Authentifizierung 9
Externe Anmeldedienste 10
Sicherheitsaudit 10
Weitere Informationen 10

MatchWare Inc.
511 West Bay Street
Suite 480
Tampa, FL 33606
United States

T: +1-813-254-6644
usa@matchware.com

MatchWare Ltd
3-5 Red Lion Street
Richmond, TW9 1RJ, UK
United Kingdom

T: +44 (0)20 8940 9700
london@matchware.com

MatchWare France
38 rue Servan
75544 Paris Cedex 11
France

T: +33 (0)810 000 172
vente@matchware.com

MatchWare GmbH
Anckelmannsplatz 1
20537 Hamburg
Deutschland

T: +49 (0) 40 543764
hamburg@matchware.com

MatchWare A/S
Thomas Koppels Gade 30
DK-8000, Aarhus C
Denmark

T: +45 86 20 88 20
aarhus@matchware.com

MATCHWARE
Software for Creative Minds

Überblick

Dieses Dokument bietet einen Überblick über das MatchWare MindView Drive.
MindView Drive ist eine Cloud-basierte Speicher- und Kollaborationsplattform, die von MindView für Windows, MindView für Mac, MindView Online und MindView Assist verwendet wird. MindView Drive basiert auf Microsoft Azure, einer Cloud-Computing-Plattform und -InfrastrGBtur, die von Microsoft erstellt und verwaltet wird. MindView Drive wurde unter Berücksichtigung von Skalierbarkeit, Verfügbarkeit, hoher Effizienz und Sicherheit entwickelt. MindView Drive wird auch als MatchWare Shared Workspace bezeichnet.

Kundendaten

Die gespeicherten Kundendaten sind:

- Nutzer E-Mail
- Name der Institution (optional)
- Nutzername (optional)

Speicherort

Kundendaten und zugehörige Metadaten, die Nutzer mit ihrem zugewiesenen Speicher verbinden, werden in einem der folgenden Microsoft Azure-Rechenzentren gehostet:

- Ost-USA (Virginia)
- Westeuropa (Niederlande)
- GB Süd (London)

Alle Daten werden im Ruhezustand verschlüsselt, um Sicherheit und Einhaltung der Vorschriften zu gewährleisten.

Zusätzlich befindet sich in Westeuropa eine zentrale gemeinsame Datenbank mit gehashten Nutzer-E-Mails und IDs. Diese Datenbank wird für schnelle Abfragen verwendet und enthält keine personenbezogenen Daten.

Der Speicherort für Kundendaten basiert standardmäßig auf dem bei der Kontoerstellung angegebenen Land. Der Standort kann optional vom Kontoadministrator über die Einstellungsseite unter https://accounts.matchware.com/ geändert werden.
Der Kundenstandort bestimmt, wo die Kundendaten gespeichert und verarbeitet werden.

Kundendaten im Transit

Alle Daten, die zwischen den Nutzern und den vorgesehenen Microsoft Azure-Rechenzentren übertragen werden, sind verschlüsselt, um Vertraulichkeit und Integrität zu gewährleisten. Verbindungen werden über Microsoft Azure Front Door verwaltet und weitergeleitet, das als sicheres Gateway dient und einen fortschrittlichen Schutz für den Nutzerverkehr bietet. Azure Front

MatchWare
Software for Creative Minds

Door nutzt HTTPS mit End-to-End-Transport Layer Security (TLS), um alle über das Netzwerk übertragenen Daten zu verschlüsseln und sie vor Abfangen oder Manipulationen zu schützen. Azure Front Door bietet eine Reihe von Sicherheitsfunktionen, die darauf ausgelegt sind, die Verbindungssicherheit zu verbessern. Dazu gehören der Schutz der Web Application Firewall (WAF) gegen häufige Schwachstellen und Angriffe, Distributed Denial of Service (DDoS)-Minderung zur Verhinderung von Servicestörungen sowie globale Lastverteilung zur Gewährleistung optimaler Leistung und Zuverlässigkeit. Darüber hinaus implementiert Azure Front Door Zugriffskontrollen, Bedrohungsinformationen und Echtzeitüberwachung, die alle zu einer robusten Sicherheitslage für Daten im Transit beitragen.
Nutzerverbindungen werden basierend auf der Geo-Position über Microsoft Azure Front Door geleitet, das Anfragen an das definierte Rechenzentrum weiterleitet.

Login-Datenfluss

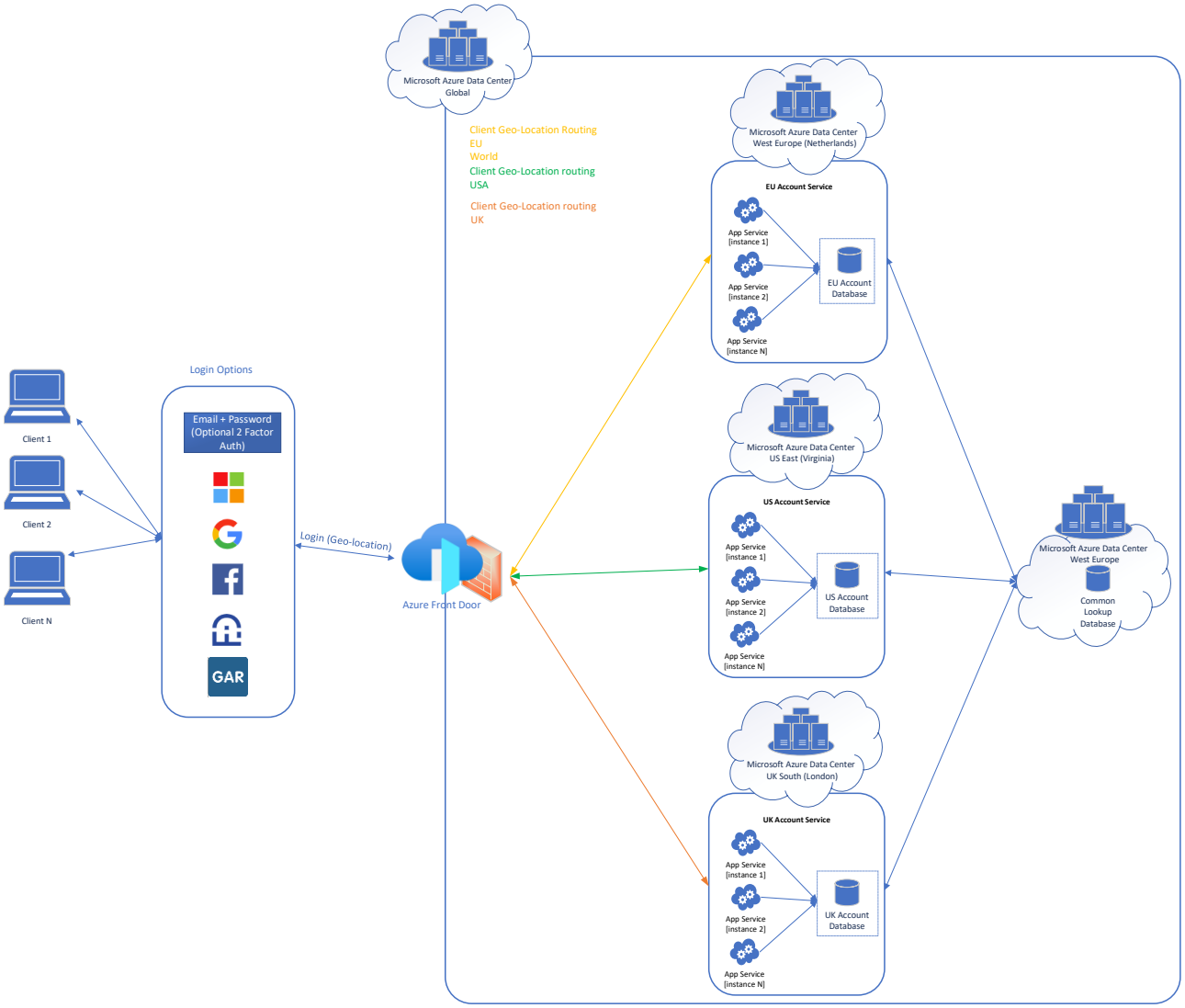

Abbildung 1 – Datenfluss während der Anmeldung

MatchWare Inc.
511 West Bay Street
Suite 480
Tampa, FL 33606
United States

T: +1-813-254-6644
usa@matchware.com

MatchWare Ltd
3-5 Red Lion Street
Richmond, TW9 1RJ, UK
United Kingdom

T: +44 (0)20 8940 9700
london@matchware.com

MatchWare France
38 rue Servan
75544 Paris Cedex 11
France

T: +33 (0)810 000 172
vente@matchware.com

MatchWare GmbH
Anckelmannsplatz 1
20537 Hamburg
Deutschland

T: +49 (0) 40 543764
hamburg@matchware.com

MatchWare A/S
Thomas Koppels Gade 30
DK-8000, Aarhus C
Denmark

T: +45 86 20 88 20
aarhus@matchware.com

Das geolokalisierungsbasierte Routing in Azure Front Door und der vom Kunden definierte Datenstandort gewährleisten eine effiziente Konnektivität und gewährleisten die Einhaltung lokaler Daten.

Beispiel für eine Anmeldung durch einen britischen Client

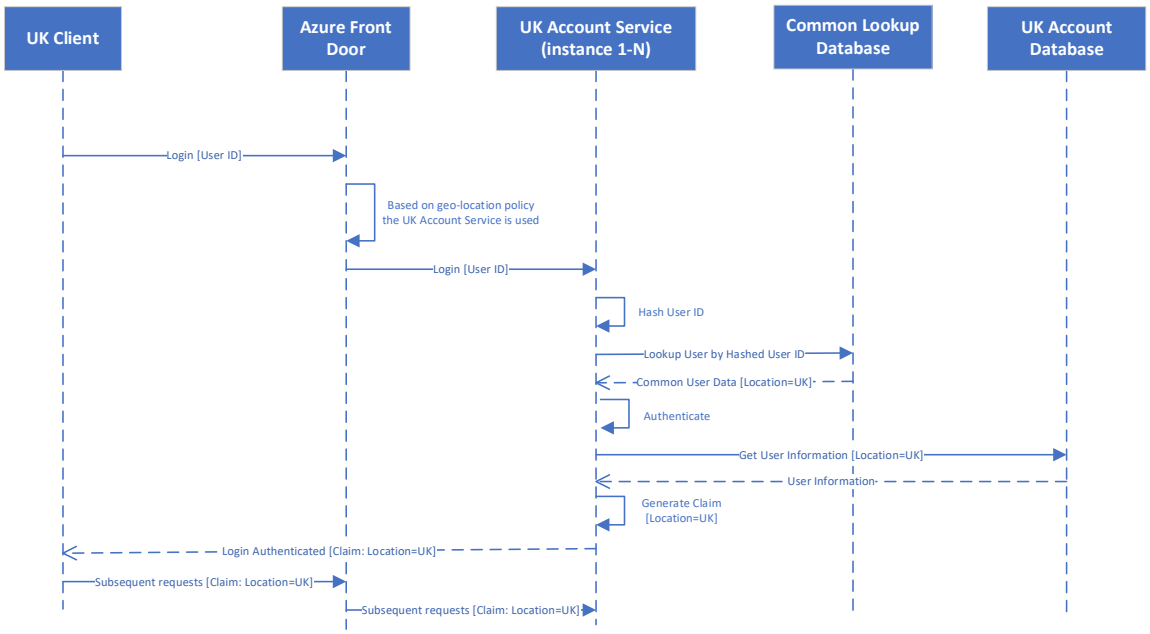

Abbildung 2 – Sequenzdiagramm eines britischen Client-Logins

Online-Dokumentenspeicherung im Ruhezustand

Alle Kundendokumentdaten werden in Microsoft Azure-Rechenzentren mithilfe von Geo Redundant Storage (GRS) gespeichert, das ein Höchstmaß an Haltbarkeit und Sicherheit bietet. Alle Daten werden im Ruhezustand im Azure-Speicher verschlüsselt. Zusätzlich werden einzelne Kundendaten mit Schlüssel pro Benutzer mithilfe der AES-256 Verschlüsselung verschlüsselt.

Benutzern wird basierend auf der ersten Anmeldung ein Standardspeicherort zugewiesen. Alternativ kann der Systemadministrator einen bestimmten Speicherort für alle Benutzer definieren. Wenn der zugewiesene Speicherort nicht korrekt ist, können die Daten an einen anderen Speicherort verschoben werden.

Die Speicherorte, die MatchWare derzeit in den Microsoft Azure-Rechenzentren zur Verfügung stellt, sind:

- Ost-USA (Virginia)
- Frankreich zentral (Paris)
- Deutschland West/zentral (Frankfurt)
- GB Süd (London)
- Westeuropa (Niederlande)

Cloud-Dienste

Alle Cloud-Services im MindView Drive-Setup nutzen verwaltete Microsoft Azure-Web-Apps, die eine robuste Skalierbarkeit und verbesserte Sicherheit gewährleisten.

Arbeitsinstanzen

Werden Dokumente aus MindView geöffnet, werden die Kundendaten sicher vom Speicherort an eine temporäre Arbeitsinstanz gesendet. Die Arbeitsinstanz behandelt den Status des Dokuments, während das Dokument geöffnet ist. Azure Traffic Manager verwendet eine geografische Standortmethode, um Benutzer basierend auf den geografischen Standorten, von denen aus sie eine Verbindung herstellen, zu bestimmten Endpunkten zu leiten. Dadurch wird sichergestellt, dass die geografisch am besten geeignete Arbeitseinheit verwendet wird, um eine effiziente Konnektivität bereitzustellen, Latenzzeiten zu reduzieren und die Einhaltung lokaler Datenschutzbestimmungen sicherzustellen (siehe Abbildung 1). Wenn das Dokument geschlossen wird, wird das aktualisierte Dokument an den richtigen Speicherort zurückgesendet und aus der temporären Arbeitsinstanz entfernt.

In jedem der folgenden Rechenzentren stehen mehrere Arbeitsinstanzen zur Verfügung, um sicherzustellen, dass die Arbeitslast skaliert wird, und um eine hohe Verfügbarkeit sicherzustellen, wenn eine oder mehrere Arbeitsinstanzen verwaltet werden.

Die derzeit von MatchWare zur Verfügung gestellten Arbeitsinstanzen befinden sich in den folgenden Microsoft Azure-Rechenzentren:

- Ost-USA (Virginia)
- Westauropa (Niederlande)
- GB Süd (London)

MatchWare
Software for Creative Minds

Datenfluss bei Online-Dokumenten

Übersicht über den Datenfluss beim Öffnen eines Online-Dokuments von einem Client aus.

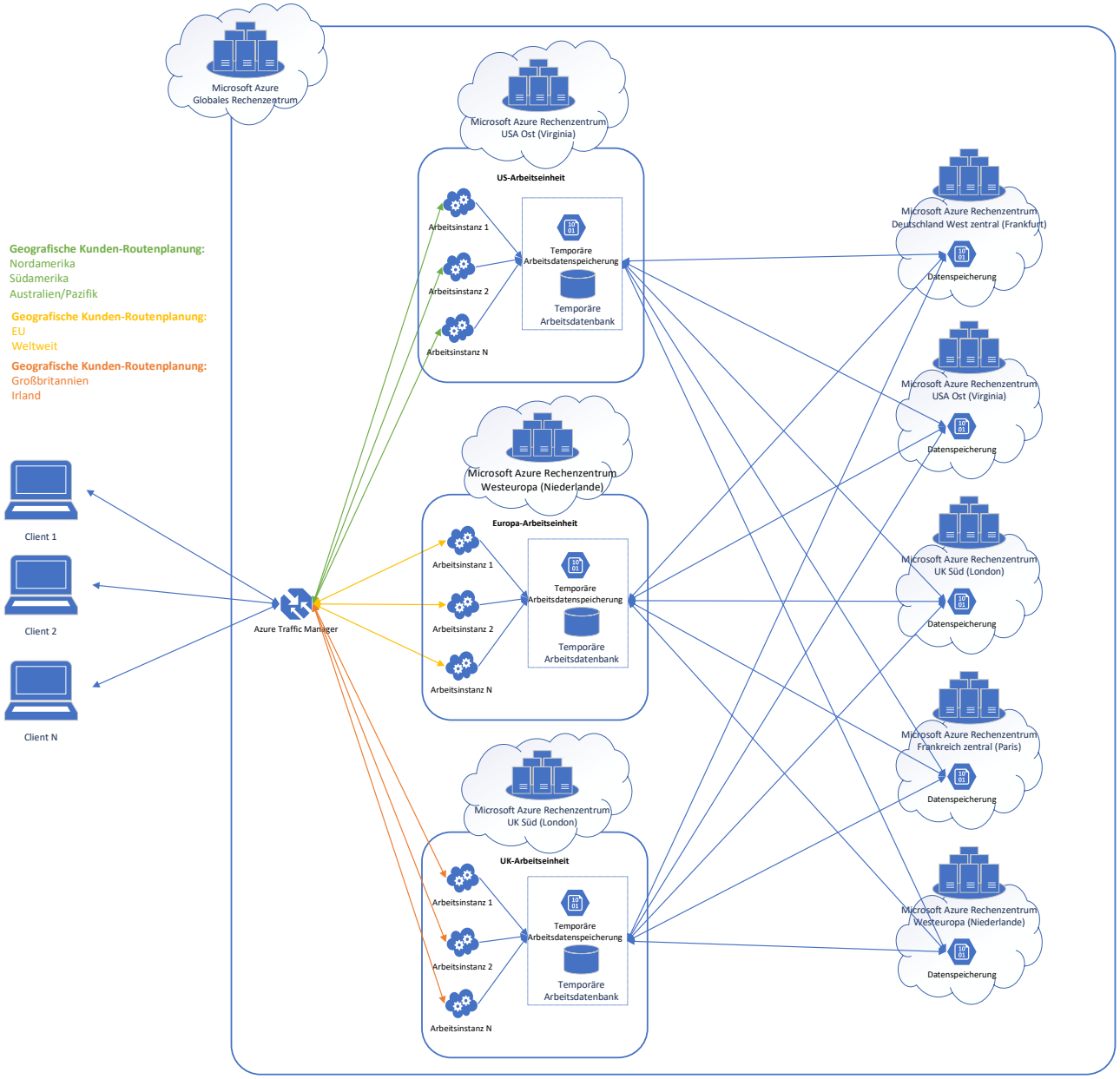

Abbildung 3 – Übersicht über den Datenfluss bei der Arbeit mit Online-Dokumenten

Azure Traffic Manager verwendet den geografischen Standort des Benutzers, um ihn basierend auf seiner Region mit der entsprechenden Arbeitseinheit zu verbinden. Das geolokalisierungsbasierte Routing gewährleistet eine effiziente Konnektivität und hält die lokale Datenkonformität aufrecht. Hier ist ein Überblick über die Geolocation-Zuordnung zu Arbeitseinheiten:

Geolokalisierung des Nutzers	Standort des Rechenzentrums
Nordamerika/Südamerika/Australien/Pazifik	Ost-USA (Virginia)
Großbritannien/Irland	GB-Süd (London)
EU, Welt	Westeuropa (Niederlande)

Hier ist ein Beispiel eines deutschen Kunden, der ein Dokument öffnet, bearbeitet und schließt.

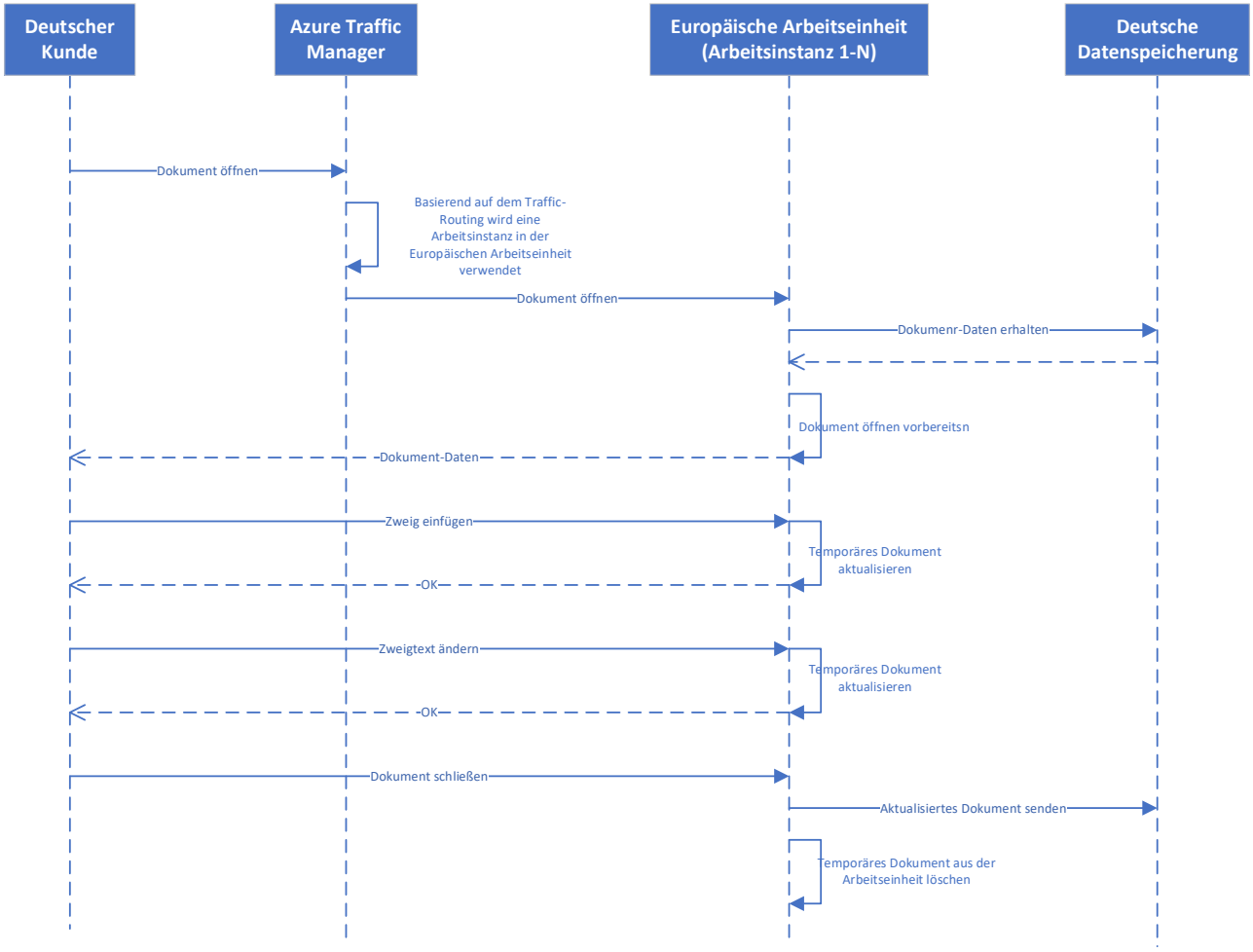

Abbildung 4 – Sequenzdiagramm eines deutschen Kunden, der ein Dokument öffnet, bearbeitet und schließt

Systemdaten im Transit

Alle internen und externen End-to-End-Verbindungen werden mit einem 256-Bit-SSL-Zertifikat (TLS 1.2) erzwungen verschlüsselt.

MATCHWARE
Software for Creative Minds

E-Mails

Vom System gesendete E-Mails verwenden den bekannten E-Mail-Dienst SendGrid von Twilio (https://sendgrid.com/), um sicherzustellen, dass sie dem höchsten Standard entsprechen.

Sicherung und Aufbewahrung

MatchWare erstellt automatisch eine 30-Tage-Sicherung aller Kundendaten. Die Sicherungsdaten werden am selben Speicherort gespeichert und verlassen niemals die Microsoft Azure-InfrastrOst-tur. Alle Sicherungsdaten werden im Ruhezustand verschlüsselt und auch mit Schlüssel pro Benutzer verschlüsselt.

Autorisierung

MindView Drive verwendet das MatchWare-Konto (https://accounts.matchware.com) für die Benutzerautorisierung. Das Autorisierungssystem verwendet das Industriestandardprotokoll OAuth2 für sichere Authentifizierungs- und Autorisierungsprozesse.

Zur weiteren Verbesserung der Sicherheit nutzt die Website Microsoft Azure Front Door, einen skalierbaren und sicheren Einstiegspunkt für die Bereitstellung von Webanwendungen mit hoher Leistung und geringer Latenz. Azure Front Door integriert DDoS-Schutz (Distributed Denial of Service) und eine Web Application Firewall (WAF), die zum Schutz vor häufigen Bedrohungen und Sicherheitsrisiken beiträgt. Dieses Setup stellt sicher, dass MindView Drive widerstandsfähig gegen böswillige Angriffe bleibt und eine sichere Umgebung für alle Benutzer bietet.

MatchWare Anmeldung

Das generische MatchWare-Login-System verwendet die E-Mail-Adresse als eindeutige Kennung und ein benutzerdefiniertes Passwort mit einer Mindestlänge von 8 Zeichen. Passwörter werden sicher als SHA256-Hash-Werte mit Salt gespeichert, um sicherzustellen, dass selbst wenn die Daten kompromittiert werden, die ursprünglichen Passwörter nicht abgerufen werden können. Das MatchWare-Konto enthält eine Richtlinie für Anmeldewiederholungen für fehlgeschlagene Anmeldeversuche, die eine Verzögerung vor dem nächsten Wiederholungsversuch zum Schutz vor Brute-Force-Angriffen einführt.

Zwei-Faktor-Authentifizierung

Die MatchWare-Anmeldung unterstützt die Zwei-Faktor-Authentifizierung (2FA) für eine zusätzliche Sicherheitsebene. Zusätzlich zur Verwendung seiner E-Mail-Adresse und seines Passworts für die Anmeldung muss der Benutzer einen Sicherheitscode eingeben, der von einer Authentifizierungs-App generiert oder per E-Mail an ihn gesendet wird.

Neben der generischen MatchWare-Anmeldung kann der Dienst auch einen oder mehrere der unterstützten externen Anmeldedienste verwenden (siehe unten).

MatchWare
Software for Creative Minds

Externe Anmeldedienste

- **Microsoft Kontoanmeldung (Office 365)**
  Das Microsoft Account (MSA) -Login ist ein generischer Microsoft Single Sign-On-Dienst. Dieser Dienst unterstützt die Multi-Faktor-Authentifizierung für mehr Sicherheit.
- **Google Kontoanmeldung**
  Das Google-Konto-Login ist ein generischer Google Single Sign-On-Dienst. Dieser Service bietet eine Bestätigung in zwei Schritten für mehr Sicherheit.
- **Facebook Anmeldung**
  Das Facebook-Login bietet eine einmalige Anmeldung für Web-, Mobil- und Desktopanwendungen. Dieser Service bietet eine Bestätigung in zwei Schritten für mehr Sicherheit.

Sicherheitsaudit

MatchWare nimmt die Sicherheit sehr ernst und bei jeder größeren Version wird ein externes Sicherheitsaudit für die gesamte Infrastruktur durchgeführt. Das Sicherheitsaudit beinhaltet auch einen Penetrationstest. Der Sicherheitsbericht kann angefordert werden.

Weitere Informationen

MindView Drive Nutzungsbedingungen
Datenschutzrichtlinie
Datensicherheitsrichtlinie