DoubleClue White Paper

1. Einführung

Die Identity & Access Management (IAM) Software DoubleClue erleichtert die Administration von Identitäten und die Verwaltung von Zugangsberechtigungen für Applikationen, Systeme und Netzwerke. Eine Multi-Faktor-Authentifizierung (MFA) mit acht verschiedenen Authentifizierungsmethoden ist das zentrale Element dieser IAM-Lösung. Zusätzlich hat DoubleClue einen integrieren CloudSafe-Speicher und eine auf KeePass basierende PasswordSafe-Funktion, mit der Benutzer ihre Passwörter verwalten können.

2. On-Premises oder gehostet in der DoubleClue.online Cloud

DoubleClue kann auf dem eigenen Server “On Premises” installiert werden und dennoch die offizielle DoubleClue App aus dem Google Play Store und App Store verwenden. Alternativ können Sie Ihr DoubleClue Cluster in der DoubleClue.online-Cloud hosten lassen. Das Setup auf DoubleClue.online dauert nur wenige Minuten.

3. Mandantenfähigkeit (Multi-Tenants)

DoubleClue ist mandantenfähig. Die Mandanten können im DoubleClue Enterprise Management (DCEM), dem zentralen Administrationstool der DoubleClue-Software, verwaltet werden:

- Verwenden Sie EINE Installation, EINE Datenbank und EINE URL für verschiedene Firmen oder Subunternehmen.
- Jeder Mandant verwendet ein eigenes Datenbankschema.
- Jeder Mandant kann seine Benutzer, Geräte, Zugriffsrechte, LDAP, RADIUS, SAML etc. vollkommen unabhängig von den anderen Mandanten verwalten.
- Alle PKIs, URLs, Ports, Clusterknoten und Diagnosetools werden in einem zentralen Verwaltungstool organisiert.
- Einzelne Mandanten können über Subdomains erreicht werden.

DoubleClue kann so als Software as a Service für mehrere Klienten eingesetzt werden. Um die Mandantenfähigkeit von DoubleClue zu nutzen, müssen Sie eine externe Datenbank verwenden. Von der integrierten Datenbank wird die Mandantenfähigkeit nicht unterstützt.

4. Zugriffsrichtlinien

Die Zugriffsrichtlinien werden in DCEM verwaltet. Sie legen fest, mit welchen Authentifizierungsmethoden, welche Benutzer Zugriff zu welchen Anwendungen und Daten haben.

4.1 Einstellungen

- Weisen Sie verschiedenen Benutzergruppen verschiedene Authentifizierungsmethoden zu.
- Verzicht auf Multi-Faktor-Authentifizierung innerhalb eines gewissen Zeitrahmens:
  Nachdem sie sich mit MFA identifiziert haben, können sich Benutzer für eine gewisse Zeit allein mit ihrem Benutzernamen und Passwort anmelden.
- Browser Fingerprint:
  Bei der Anmeldung mit MFA wird ein einzigartiger Browser Fingerprint berechnet, um den verwendeten Browser / das verwendete Device eindeutig zu identifizieren. Die Benutzer können sich für eine gewisse Zeit mit ihrem Benutzernamen und Passwort, ohne MFA, anmelden, wenn der verwendete Browser Fingerprint mit dem des vorherigen Logins übereinstimmt.
- Network Bypass:
  Legen Sie im Network Bypass bestimmte sichere Netzwerkbereiche fest. Wenn sich ein Benutzer aus einem dieser Netzwerkbereiche anmeldet, können Sie sich mit ihrem Benutzernamen und Passwort anmelden, ohne MFA verwenden zu müssen. DoubleClue unterstützt IPv4 und IPv6.
- Wahl der Authentifizierungsmethode:
  Aktivieren und deaktivieren Sie Authentifizierungsmethoden für verschiedene Benutzergruppen. Es ist möglich, mehrere Authentifizierungsmethoden für eine Benutzergruppe zu aktivieren.
- Standardauthentifizierungsmethode:
  Legen Sie eine Standardauthentifizierungsmethode für eine bestimmte Benutzergruppe fest. Benutzer können andere Authentifizierungsmethoden verwenden, die für ihre Gruppe aktiviert wurden, indem Sie ein Präfix vor ihren Anmeldenamen setzen.

4.2 Zugriffsrichtlinien zuweisen

Zugriffsrichtlinien können verschiedenen Anwendungstypen (RADIUS, SAML, Rest-Webservices etc.), Anwendungen (Cisco Meraki, Citrix ShareFile, Dropbox etc.) und Benutzergruppen zugewiesen werden.

Die Anwendung der zugewiesenen Zugriffsrichtlinien folgt der folgenden Hierarchie:

a) Wenn ein Benutzer Mitglied einer bestimmten Gruppe ist und dieser Gruppe eine Zugriffsrichtlinie speziell für diese Anwendung oder diesen Anwendungstypen zugewiesen wurde, wird diese Zugriffsrichtlinie verwendet.
b) Wenn ein Benutzer Mitglied einer bestimmten Gruppe ist und dieser Gruppe eine allgemeine Zugriffsrichtlinie zugewiesen wurde, wird diese Richtlinie verwendet.
c) Wenn ein Benutzer Mitglied mehrerer Gruppen ist und diesen Gruppen verschiedene Zugriffsrichtlinien zugewiesen wurden, wird die Zugriffsrichtlinie verwendet, der über DCEM die höchste Priorität zugewiesen wurde.
d) Wenn ein Benutzer ein Mitglied einer Gruppe ist, der keine Zugriffsrichtlinie zugewiesen wurde, oder wenn der Benutzer nicht in einer Gruppe ist, wird die Zugriffsrichtlinie verwendet, die der entsprechenden Anwendung zugewiesen wurde.
e) Wenn einer Anwendung keine Zugriffsrichtlinie zugewiesen wurde, wird die Zugriffsrichtlinie des Anwendungstypen verwendet.
f) Wenn einem Anwendungstypen keine Zugriffsrichtlinie zugewiesen wurde, wird die “Globale Zugriffsrichtlinie” angewendet.

4.3 Globale Zugriffsrichtlinie

Wenn wie oben beschrieben einer Anwendung oder einer Benutzergruppe keine Zugriffsrichtlinie zugewiesen wurde, verwendet DCEM die „Globale Zugriffsrichtlinie“. Die „Globale Zugriffsrichtlinie“ wird während der DoubleClue-Installation automatisch mit Standardwerten angelegt. Nach der Installation kann die globale Zugriffsrichtlinie in DCEM angepasst aber nicht gelöscht werden. In einem Szenario mit mehreren Mandanten hat jeder Mandant seine eigene globale Zugriffsrichtlinie.

5. Authentifizierungsmethode

DoubleClue unterstützt zurzeit acht verschiedene Authentifizierungsmethoden. Dies erlaubt es Administratoren und Benutzern auszuwählen, welche Methode am besten für Ihre Situation und Vorlieben geeignet ist. Weitere Authentifizierungsmethoden werden in Zukunft hinzugefügt.

5.1 Push Approval

Push Approval ist die sicherste Authentifizierungsmethode von DoubleClue. Sie basiert auf einem PKI Private Key 2048 Bit Zertifikat. Benutzer erhalten eine Push Notification auf Ihrem Smartphone. Nachdem Sie sich in Ihre DoubleClue-App eingeloggt haben, können Sie die erhaltenen Benachrichtigungen und Transaktionen annehmen oder ablehnen. Push Approvals verwenden HTML-formatierte, vorkonfigurierte Vorlagen mit Platzhaltern. Die Antworten werden digital signiert und vom DoubleClue Enterprise Management verifiziert.

5.2 QR-Code Approval

Diese Ein-Klicke-Authentifizierungsmethode basiert auf einem PKI Private Key 2048 Bit Zertifikat und einem zufälligen AES-256 Verschlüsselungsalgorithmus. Benutzer identifizierenden sich, in dem sie den QR-Code mit ihrer DoubleClue-App scannen. Der QR-Code-Schlüssel ist normalerweise für 2 Minuten gültig.

5.3 FIDO U2F und FIDO2 Token

FIDO ist ein offener Standard für Multi-Faktor-Authentifizierung. FIDO Security Keys sind physische Tokens, die sich über Bluetooth oder USB mit einem Gerät verbinden. FIDO2 integriert zusätzlich die biometrische Authentifizierung mit Fingerabdruck für noch mehr Sicherheit. Weitere Information finden Sie auf https://fidoalliance.org/.

5.4 OTP Token

OTP Tokens sind Hardware Tokens, die bei jedem Login ein Einmalpasswort generieren. Der Benutzer gibt das Einmalpasswort zusammen mit seinem Benutzerpasswort ein. DoubleClue unterstützt den Token Type “**TIME_6_SHA1_60**”. Dies ist ein zeitbasiertes OTP mit 6 Zahlen, das einen SHA1-Algorithmus und ein Zeitfenster von 60 Sekunden verwendet.

5.5 DoubleClue Passcode

Wenn keine Internetverbindung verfügbar ist, können Benutzer mit ihrer DoubleClue einen Offline-Passcode generieren.

5.6 Passwort

Ein Benutzer kann sich nur mit seinem Benutzernamen und Passwort anmelden. Diese klassische Identifizierungsmethode ist für Anwendungen in bestimmten, sicheren Netzwerken gedacht, in denen MFA nicht benötigt wird.

5.7 SMS

Ein zufälliger Passcode wird erstellt und Benutzer via SMS zugeschickt. Der SMS Passcode wird ohne Verschlüsselung übertragen. Diese Methode wird normalerweise zusätzlich zum Login mit Passwort verwendet.

5.8 Voice Message

Ein zufälliger Passcode wird erstellt und dem Benutzer mittels Anruf via Festnetz- oder Mobiltelefon geschickt. Der Passcode wird unverschlüsselt übertragen.

6. DoubleClue App

6.1 Universal DoubleClue App

Die Standard-DoubleClue-App steht für Android, iOS, Windows Desktop, MAC und Linux zur Verfügung. Sie kann vom Google Play Store oder App Store heruntergeladen werden. Bitte kontaktieren Sie support@doubleclue.com für Versionen für weitere Operationssysteme.

Nach der Installation können Sie die App aktiveren, indem Sie den Benutzernamen, das Passwort und einen Aktivierungscode eingeben. Während des Aktivierungsprozesses wird ein Private Key generiert. Der Private Key verlässt das Smart Device niemals und wird auf ihm in verschlüsselter Form gespeichert. Sämtliche Transaktionen der App werden digital signiert.

Bei der Installation identifiziert DoubleClue die einzigartige DNA des Smart Devices. Die aktivierte App funktioniert nur auf dem entsprechenden Gerät. Sie kann nicht auf ein anderes Gerät geklont werden.

Benutzer können die DoubleClue-App auf verschiedenen Plattformen installieren und aktivieren. Eine App die auf einem Gerät installiert und aktiviert wurde, kann von mehreren Benutzern verwendet werden.

App-Vorrausetzungen:

- Android: Version 5.0 (Android Lollipop) oder neuer
- Windows: Version 7, 8, 10
- iOS: Version 10.0 oder neuer

6.2 DoubleClue SDK-Bibliothek für Android und iOS

Die DoubleClue-App besteht aus einer DoubleClue-SDK-Bibliothek und der App-GUI. Mit Hilfe der SDK-Bibliothek können DoubleClue-Features in Ihre eigene App integriert werden.

7. Integration von Anwendungen mit DoubleClue

DoubleClue unterstützt Anwendungen von Drittanbietern über die folgenden Schnittstellen:

- REST Web-Services
- RADIUS
- SAML
- OpenID-OAuth
- Auth-Connector
- RD Web Access (via plugin)
- ADFS Plugin
- Windows Login Credential Provider

8. DoubleClue Enterprise Management (DCEM)

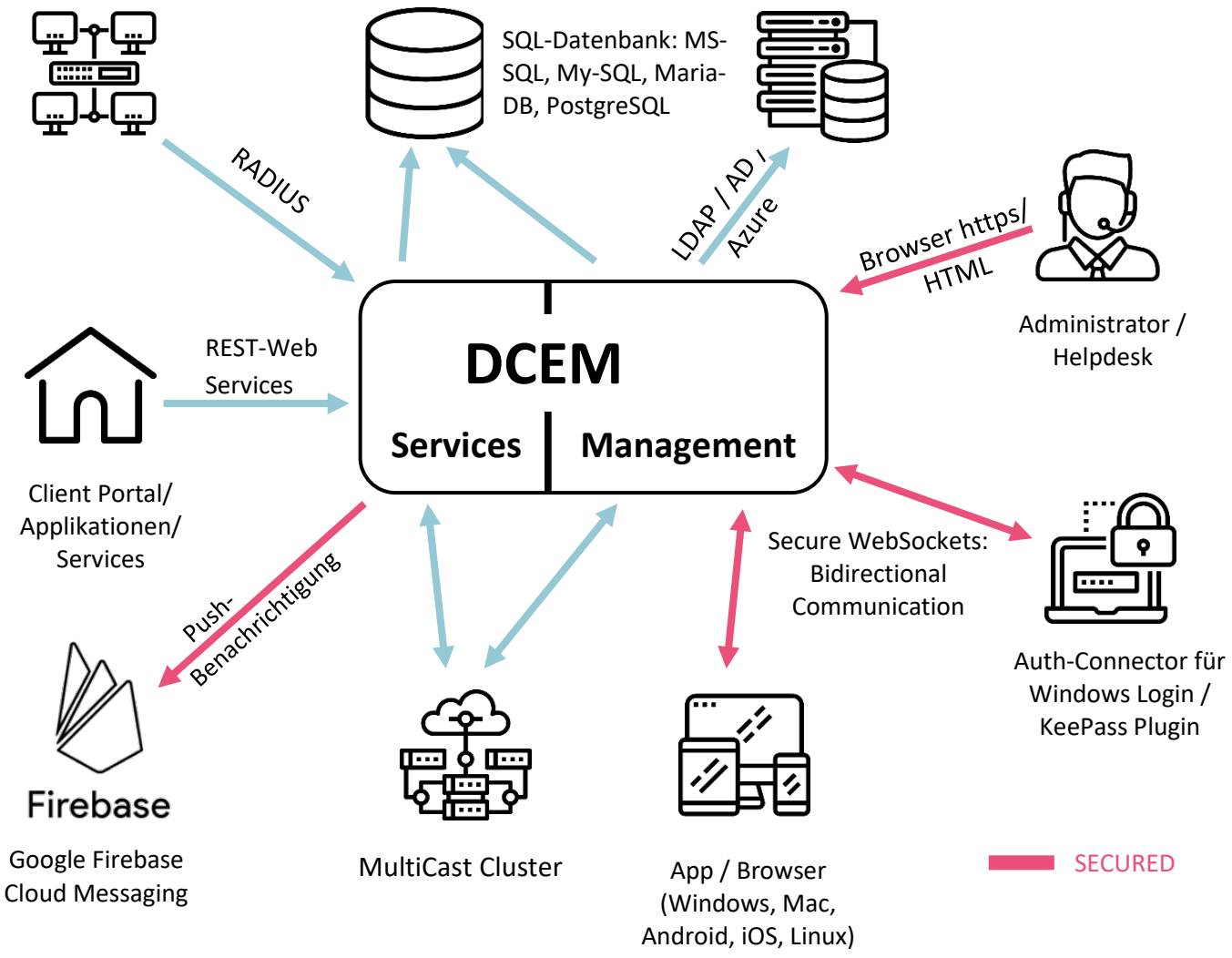
8.1 Übersicht der Funktionen

- Zentrale Verwaltung von Benutzern, Geräten, Administratoren, Zugriffsrichtlinien, Mandanten etc.
- DoubleClue Enterprise Management kann auf einem lokalen Server (on Premises) installiert oder auf doubleclue.online gehostet werden.
- Hoher Schutz vor Ausfällen durch eine redundante Serverstruktur und Lastverteilung durch skalierbare Clusterknoten. Der benötigte Load Balancer ist nicht Teil der DoubleClue-Lösung.
- Genau abgestimmte, rollenbasierte Zugriffsrechte für Administratoren
- Aufzeichnung aller Änderungen
- Integration und Kommunikation mit Firmenanwendungen über die oben genannten Schnittstellen
- Kommunikation mit der DoubleClue-App über sichere Websockets
- Verwendung einer eigenen PKI zur Kommunikation mit der DoubleClue-App. Darum ist die App unabhängig von der PKI des Betriebssystems.
- Eigene eingebaute Certificate Authority mit Unterstützung für externe CAs
- Unterstützung einer eingebauten Datenbank (“Embedded Databse”) sowie der externen Datenbanken Maria DB, MySQL, MS SQL und PostgreSQL
- Läuft auf Windows und Linux

- Volle Active Directory Integration (Domains, Benutzer und Gruppen aus Active Directory, Azure AD und LDAP)
- Unterstützt Infrastrukturen mit mehreren Domänen

8.2 Struktur

DCEM ist ein Cluster, das aus verschiedenen verbundenen unabhängigen Servern besteht. Es ist die zentrale Komponente der DoubleClue-Plattform.
DCEM ist in verschiedene Bereiche unterteilt. Das folgende Szenario zeigt alle möglichen Komponenten von DCEM und die Bereiche mit denen sie kommunizieren:

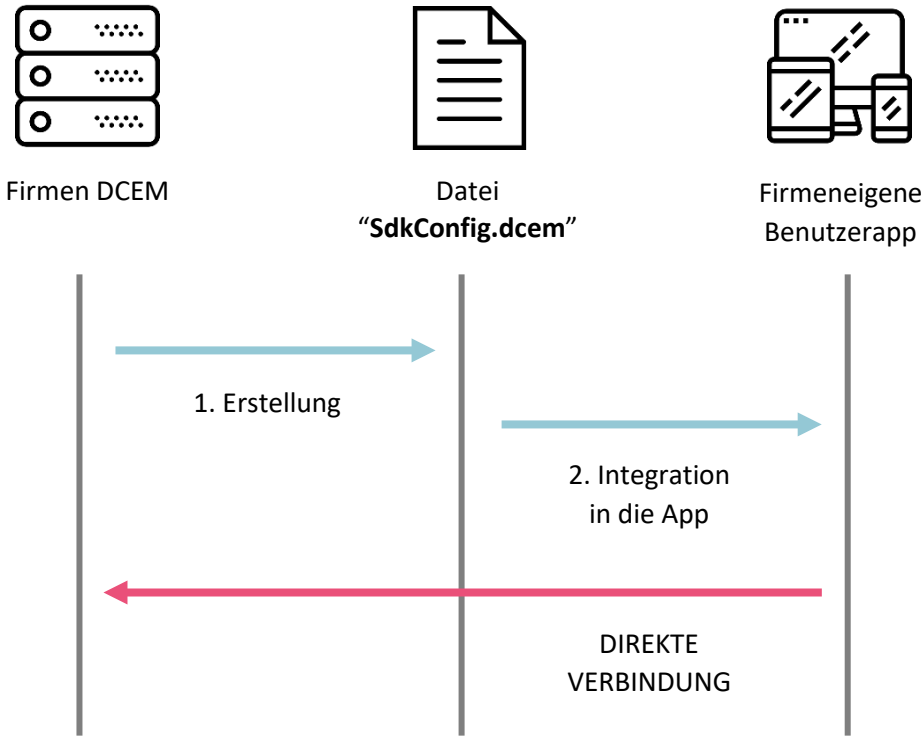


8.3 Verbindungsszenarios

Die DoubleClue-App kann sich direkt oder über den DoubleClue-Dispatcher mit DCEM verbinden.

8.3.1 Direkte Verbindung mit der In-House App

Die App verbindet sich direkt mit der Firmen-DCEM-Installation. Um diesen Verbindungstypen zu benutzen, müssen Sie eine eigene App erstellten und die DCEM-Zertifikate in sie integrieren.



8.3.2 Verbindung über den DoubleClue-Dispatcher

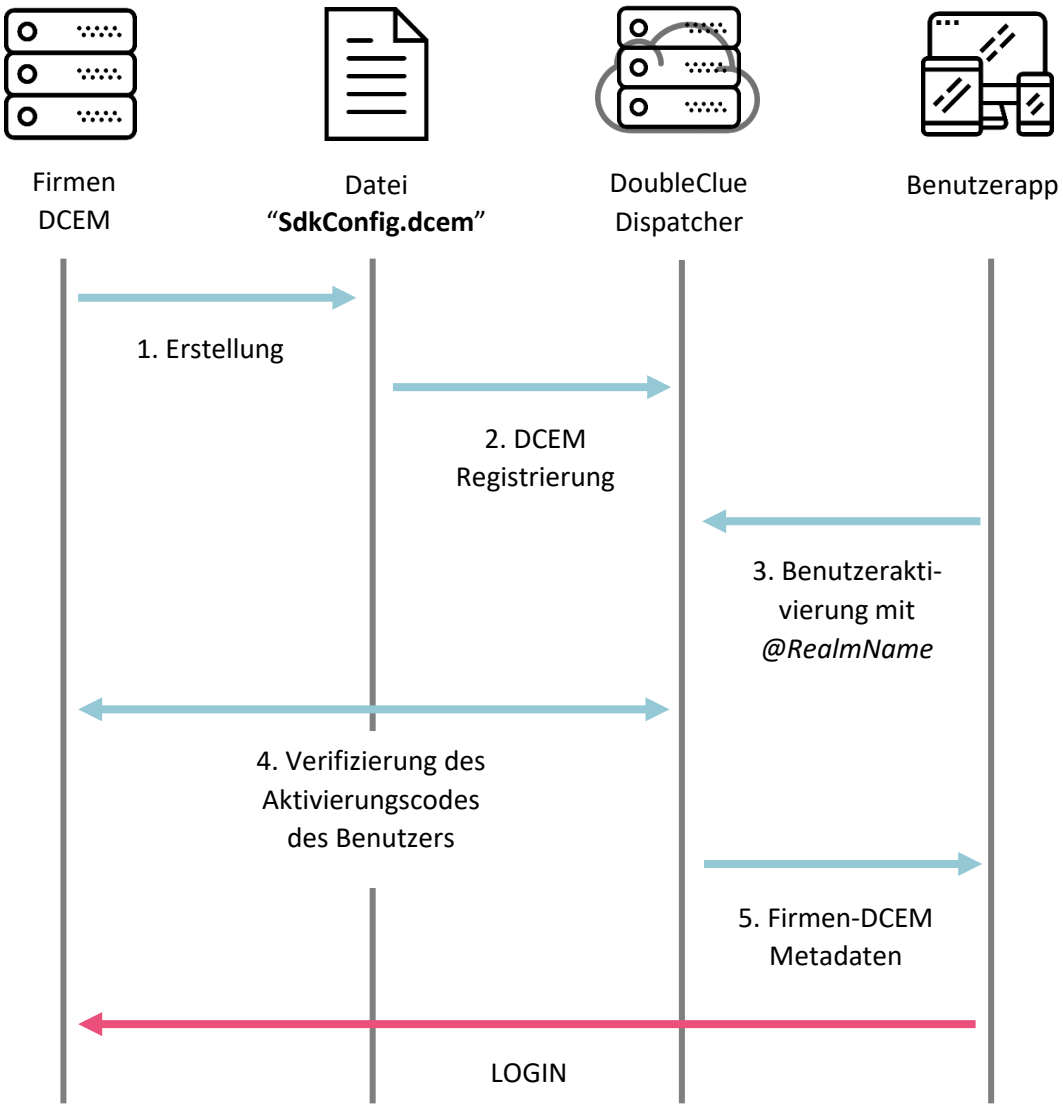
Dieser Verbindungtyp erlaubt die Verwendung der allgemeinen DoubleClue-App. Um ihn zu verwenden, muss das installierte DCEM beim globalen DoubleClue-Dispatcher registriert werden.

⚠ Voraussetzung: DCEM Port 443 muss vom Internet aus erreichbar sein. Bitte passen Sie Ihre Firewalleinstellungen entsprechend an.

Außerdem ist es notwendig, dass das DCEM-Cluster ein Domain Name System (DNS) hat und der Secure WebSocket-Port vom Internet aus erreichbar ist.

Der DoubleClue-Dispatcher ist ein DCEM-Cluster in der Cloud, das von der *HWS Informationssysteme GmbH* verwaltet wird. Wenn ein Smartgerät aktiviert wird, verifiziert der Dispatcher die Login-ID und

den Aktivierungscode mit der Domain der „DCEM-Installation“. Wenn der Aktivierungscode gültig ist, schickt der Dispatcher die DCEM SDK Konfigurations-Metadatendatei an das Gerät. Beim Anmelden verbindet sich das Gerät daraufhin direkt mit der Firmen-DCEM-Installation.



8.3.3 Verbindung mit DoubleClue-Dispatcher über Reverse-Proxy

Für Testzwecke können Sie eine Verbindung mit dem DoubleClue-Dispatcher über Revers-Proxy herstellen. In diesem Szenario verbindet sich Ihr DCEM mit dem DoubleClue Reverse-Proxy und alle Daten gehen durch einen Tunnel zwischen Ihrem DCEM und DoubleClue Reverse-Proxy. Es ist darum nicht nötig, einen Listening-Port in Ihrer Firewall zu öffnen.

8.4 Benutzerrollen

Benutzern kann eine von mehreren verschiedenen Rollen zugewiesen werden. Diese Rollen können von den DoubleClue-Administratoren frei angepasst oder neu erstellt werden. Benutzerrollen können

für jeden Mandanten individuell eingestellt werden. Sie erstrecken sich vom einfachen Benutzer, der keinen Zugang zu DCEM hat, über verschiedene Ränge von Administratoren für verschiedene Schnittstellen bis hin zum Superadministrator mit Zugriff auf die komplette DoubleClue-Infrastruktur. Für einzelne Mandanten können unterschiedliche Rollen angelegt werden.

9. Benutzerfunktionen

9.1 UserPortal

DoubleClue UserPortal ist ein Self-Service-Portal für DoubleClue-Benutzer. Es erlaubt es Benutzern, sich selbst zu registrieren und die Smart Devices, FIDO-Token und OTP-Token, die mit ihrem DoubleClue-Account verbunden sind, selbstständig ohne die Hilfe eines Administrators zu verwalten. Über UserPortal erhalten Benutzer außerdem Zugang zu PasswordSafe und CloudSafe.

Die unterschiedlichen Bereiche und Aktionen, die in UnserPortal zur Verfügung stehen, können von den Administratoren vollkommen frei eingerichtet werden. Es ist außerdem möglich, zwei verschiedene Arten von Zugriffen festzulegen: Einen eingeschränkten Zugriff, wenn sich der Benutzer nur mit seinem Passwort anmeldet, und einen erweiterten Zugriff, wenn er sich mit MFA anmeldet.

9.2 PasswordSafe

DoubleClue PasswordSafe ist ein Passwortmanager, der es ermöglicht, Benutzerpasswörter in der DoubleClue-Infrastruktur zu speichern und zu verwalten. Er schützt die Passwörter mit DoubleClue-Multi-Faktor-Authentifizierung und versichert zugleich, dass sie jederzeit einfach von den Benutzern erreicht werden können. Die Passwörter können in der DoubleClue App oder über die UserPortal Web UI verwaltet werden. Die Passwortdateien werden dabei nie lokal auf einem Gerät gespeichert. Außerdem ist ihr Format kompatibel mit KeePass.

9.2.1 KeePass Plugin

Das DoubleClue KeePass Plugin erlaubt es, PasswordSafe-Dateien einfach und schnell vom Windows Desktop in den PasswordSafe herauf- oder herunterzuladen. Es ist kompatibel mit KeePass Password Safe 2.4.0 oder höher.

9.3 CloudSafe

DoubleClue CloudSafe ist ein Cloudspeicher für wichtige und vertrauliche Dateien und Dokumente. Er ist durch DoubleClue UserPortal erreichbar. Dateien in CloudSafe werden durch die DoubleClue MFA und eine AES-Verschlüsselung geschützt. DoubleClue-Benutzer können die Dateien mit anderen Benutzern des gleichen Mandanten teilen.

Es ist außerdem möglich, einzelne Dateien mit einem zusätzlichen Passwort zu schützen. Dadurch werden die Daten durch eine weitere Verschlüsselung mit Salts geschützt.

10. DoubleClue Credential Provider

DoubleClue Credential Provider beschützt Windows 10 Betriebssysteme mit DoubleClue MFA. Es handelt sich um ein zusätzliches Softwarepaket, das auf dem Windows-Host-System installiert wird. Nach der Installation ersetzt es das Standard-Windows-Login und überlässt es DCEM, den Authentifizierungsprozess abzuwickeln.

DoubleClue Credential Provider unterstützt sechs der DoubleClue Multi-Faktor-Authentifizierungsmethoden. Ihre Verfügbarkeit kann in den Zugriffrichtlinien genauer definiert werden. Wenn Sie den Benutzern den Zugriff erleichtern möchten, wenn Sie sich aus einem sicheren Netzwerk, zum Beispiel einem Firmennetzwerk, anmelden, können Sie außerdem DoubleClue Confidential Network Server (CNS) nutzen. Dabei handelt es sich um einen Service im Hintergrund, der es Benutzern erlaubt sich mit Ihrem Benutzernamen und Passwort anzumelden, wenn Sie sich über einen sicheren Netzwerkserver anmelden.