XignSys

Leistungs-beschreibung

XignSys GmbH

Stand: September 2021

Inhaltsverzeichnis

1. Produktvarianten

Die XignSys GmbH (im Nachfolgenden: XignSys) bietet ihren Kunden mit der **XignIn-Technologie** eine nutzerfreundliche, sichere und flexible Lösung zur Authentifizierung gegenüber Anwendungen aus der digitalen und realen Welt.

Die XignIn-Technologie basiert auf digitalen Zertifikaten und Signaturen, sowie modernsten kryptografischen Verfahren und löst damit herkömmliche, sicherheitskritische Authentifizierungsmethoden wie etwa Nutzername/Passwort, Einmal-TANs und kostspielige Hardware (Tokens/Schlüsselkarten) nachhaltig ab.

Die zentrale Komponente ist der **XignIn-Manager**. Er stellt grundsätzlich eine Trusted Third Party dar, um das Vertrauen zwischen dem Identity Provider, einem berechtigten Diensteanbieter und der Nutzer:in zu ermöglichen. Standardmäßig nimmt der XignIn-Manager darüber hinaus die Rolle einer Access Management Lösung mit entsprechender Funktionalität ein und kann zusätzlich als Identity Management Lösung genutzt werden.

Das nutzereigene Smartphone in Kombination mit der barrierefreien **Xign.Me-App** dient als passwortloses Authentifizierungs-Tool und gewährleistet maximale Nutzerfreundlichkeit. Die App ist in der Lage unterschiedlichste Einstiegspunkte zu verarbeiten, um eine Authentifizierung durchführen zu können.

Zusätzliche Technologien zur automatisierten Datenerfassung im Kontext von Erstidentifikationsverfahren oder zur Umsetzung von Use Cases mit spezifischen Anforderungen und Voraussetzungen, wie etwa im physischen Anwendungsbereich, können über Technologiepartner bezogen werden.

Es gelten die Endkunden-Lizenzbedingungen (Stand: Juli 2021) der XignSys.

1.1 SaaS

1.1.1 Xign.Me as a Service (empfohlen)

Die Produktvariante **Xign.Me as a Service** setzt sich aus folgenden Komponenten zusammen:

Server:	XignIn-Manager (Trusted Third Party & Identity und Access Management)
App:	Xign.Me-App (Nutzerseitiges Authentifizierungs-Tool)

Mit Xign.Me as a Service profitieren Sie direkt von der schnellen und unkomplizierten Inbetriebnahme, den geringen Betriebskosten und einem professionellen Datenmanagement in zertifizierten Rechenzentren.

Die Nutzung wird verbrauchsabhängig entsprechend dem vereinbarten Pay-per-User-Modell fakturiert.

Im Rahmen der technischen und betrieblichen Möglichkeiten erbringt die XignSys die in der untenstehenden Produktmatrix dargestellten Leistungen. Eine genaue Beschreibung dieser Leistungen ist in den entsprechenden Kapiteln zu finden.

Xign.Me as a Service	
Anbindung (siehe Kapitel 2)	
JS Login (embedded)	+ (Einbettung durch Kunden)
OIDC	+
SAML	€ (auf Anfrage)
User Onboarding (siehe Kapitel 3)	
via App	+
via XignIn-Manager	+
Remote via Remote Registration API	€
Remote via OIDC	+
Identity- und Access Management (siehe Kapitel 4)	
Ein-Faktor-Authentifizierung	+
Zwei-Faktor-Authentifizierung	+
Multi-Faktor-Authentifizierung	€

Variable Authentifzierungsfaktoren	€
Autorisierung und Rollen	+
Self-Service: Globale Administration	-
Self-Service: Organisationen	
Multiple Dienste	+
Nutzer:innen & Rechte	+
Self-Service: Dienste	
Regulierung erforderlicher Daten	+
Nutzer:innen & Rechte	+
Rollen	+
Restriktiver Zugriff	+
Verschlüsselung	+
Self-Service: Nutzer:innen	+
Remote Management (bspw. KeyCloak)	€€ (auf Anfrage)
Usability (siehe Kapitel 5)	
Ganzheitlich optimierte und konsistente User Experience	+
Barrierefreie App nach WCAG 2.1 Level AA+	+
Orts- und zeitunabhängige Authentifizierung	+
Multiple Geräte	+
Nachtragen fehlender erforderlicher Datenattribute während Authentifizierung	+
Flexibilität und Anpassungsfähigkeit (siehe Kapitel 6)	
Standard Einstiegspunkte Authentifizierung (QR-Code, Intent/Custom URL)	+
Premium Einstiegspunkte Authentifizierung	€(€) (auf Anfrage)

(Push, NFC, Bluetooth, WLAN, RFID, Sound)	
XignIn-Manager als Identity Provider	+
Kundeneigener Identity Provider (via OIDC)	+
Custom Branding für Endnutzer	
Login via JS Login	+
Login via OIDC	-
App	-
E-Mails	-
Erweiterbarkeit (siehe Kapitel 7)	
Kontextbasierte Authentifizierungsfaktoren (Verhalten, Standort, Handeln)	€ (auf Anfrage)
InApp-Authentifizierung	-
Multiple Apps	-
KYC	€ (auf Anfrage)
Spezifische Anforderungen	€€ (auf Anfrage)
Sicherheit und Datenschutz (siehe Kapitel 8)	
Passwortlose Authentifizierung	+
Digitale Zertifikate	+
Starke Verschlüsselung	+
Nutzerdaten	+
Datentransparenz	+
Zertifizierungen und Prüfberichte	+
Produktsupport (siehe Kapitel 9)	
Sicherheits-Updates	+
Produkt-Updates/-Upgrade	+
Störungsbeseitigung	+

	Service Level & Verfügbarkeit	+
	Support Level Bronze	+
	Support Level Silber	€
	Support Level Gold	€€
	Zusätzliche Dienstleistungen (bspw. Consulting, Schulungen, Aufbau eines Identity Management Systems, Identity Management als Managed Service)	€(€) (auf Anfrage)

+	Leistung in der Produktvariante enthalten
-	Leistung in der Produktvariante nicht enthalten
€	Leistung gegen zusätzliches Entgelt in der Produktvariante zubuchbar

1.1.2 XignIn as a Service

Die Produktvariante **XignIn as a Service** setzt sich aus folgenden Komponenten zusammen:

Server:	XignIn-Manager (Trusted Third Party & Identity und Access Management)
App:	Kunden-App mit integriertem XignIn-SDK (Nutzerseitiges Authentifizierungs-Tool)

Mit XignIn as a Service haben Sie die Möglichkeit, die XignIn-Technologie in Ihre eigene App zu integrieren. Der XignIn-Manager bleibt als Trusted Third Party und IAM in Form einer SaaS-Lösung bestehen. So profitieren Sie in diesem Kontext weiterhin von der schnellen und unkomplizierten Inbetriebnahme, den geringen Betriebskosten und einem professionellen Datenmanagement in zertifizierten Rechenzentren.

Die Nutzung wird verbrauchsabhängig entsprechend dem vereinbarten Pay-per-User-Modell fakturiert.

XignIn as a Service	
Anbindung (siehe Kapitel 2)	
JS Login (embedded)	+ (Einbettung durch Kunden)
OIDC	+
SAML	€ (auf Anfrage)
User Onboarding (siehe Kapitel 3)	
via App	Abhängig von app-seitiger Umsetzung des Kunden
via XignIn-Manager	+
Remote via Remote Registration API	€
Remote via OIDC	+
Identity- und Access Management (siehe Kapitel 4)	
Ein-Faktor-Authentifizierung	+
Zwei-Faktor-Authentifizierung	+
Multi-Faktor-Authentifizierung	€
Variable Authentifzierungsfaktoren	€
Autorisierung und Rollen	+

Self-Service: Globale Administration	-
Self-Service: Organisationen	
Multiple Dienste	+
Nutzer:innen & Rechte	+
Self-Service: Dienste	
Regulierung erforderlicher Daten	+
Nutzer:innen & Rechte	+
Rollen	+
Restriktiver Zugriff	+
Verschlüsselung	+
Self-Service: Nutzer:innen	+
Remote Management (bspw. KeyCloak)	€€ (auf Anfrage)
Usability (siehe Kapitel 5)	
Ganzheitlich optimierte und konsistente User Experience	Abhängig von app-seitiger Umsetzung des Kunden
Barrierefreie App nach WCAG 2.1 Level AA+	Abhängig von app-seitiger Umsetzung des Kunden
Orts- und zeitunabhängige Authentifizierung	+
Multiple Geräte	+ (via XignIn-Manager) Via App: Abhängig von app-seitiger Umsetzung des Kunden
Nachtragen fehlender erforderlicher Datenattribute während Authentifizierung	Abhängig von app-seitiger Umsetzung des Kunden
Flexibilität und Anpassungsfähigkeit (siehe Kapitel 6)	
Standard Einstiegspunkte Authentifizierung (QR-Code, Intent/Custom URL)	+
Premium Einstiegspunkte Authentifizierung	€(€) (auf Anfrage)

(Push, NFC, Bluetooth, WLAN, RFID, Sound)	
XignIn-Manager als Identity Provider	+
Kundeneigener Identity Provider (via OIDC)	+
Custom Branding für Endnutzer	
Login via JS Login	+
Login via OIDC	-
App	+
E-Mails	-
Erweiterbarkeit (siehe Kapitel 7)	
Kontextbasierte Authentifizierungsfaktoren (Verhalten, Standort, Handeln)	€ (auf Anfrage)
InApp-Authentifizierung	Abhängig von app-seitiger Umsetzung des Kunden
Multiple Apps	€
KYC	€ (auf Anfrage)
Spezifische Anforderungen	€€ (auf Anfrage)
Sicherheit und Datenschutz (siehe Kapitel 8)	
Passwortlose Authentifizierung	+
Digitale Zertifikate	+
Starke Verschlüsselung	+
Nutzerdaten	+
Datentransparenz	Abhängig von app-seitiger Umsetzung des Kunden
Zertifizierungen und Prüfberichte	- (Nicht im Verantwortungsbereich der XignSys)
Produktsupport (siehe Kapitel 9)	
Sicherheits-Updates	+ (XignIn-Manager) App: SDK-Updates sind je nach Vereinbarung vom Kunden zu berücksichtigen und umzusetzen

	Produkt-Updates/-Upgrade	+ (XignIn-Manager) App: SDK-Updates sind je nach Vereinbarung vom Kunden zu berücksichtigen und umzusetzen
	Störungsbeseitigung	+
	Service Level & Verfügbarkeit	+
	Support Level Bronze	+
	Support Level Silber	€
	Support Level Gold	€€
	Zusätzliche Dienstleistungen (bspw. Consulting, Schulungen, Aufbau eines Identity Management Systems, Identity Management als Managed Service)	€(€) (auf Anfrage)

+	Leistung in der Produktvariante enthalten
-	Leistung in der Produktvariante nicht enthalten
€	Leistung gegen zusätzliches Entgelt in der Produktvariante zubuchbar

1.2 XignIn Private

Die Produktvariante **XignIn Private** setzt sich aus folgenden Komponenten zusammen:

Server:	XignIn-Manager Self-Hosted oder Managed in Private Cloud (Trusted Third Party & Identity und Access Management)
App:	Kunden-App mit integriertem XignIn-SDK (Nutzerseitiges Authentifizierungs-Tool)

Mit XignIn Private haben Sie die uneingeschränkte Kontrolle, sind dabei vollständig flexibel, autonom und können die Lösung in höchstem Maße individualisieren.

Die Produktvariante XignIn Private wird auf der Hardware des Kunden oder „Managed“ in einer Private Cloud realisiert. Die notwendigen Serverleistungen sind vom Kunden gesondert bereitzustellen. Die XignSys stellt dem Kunden eine Auflistung mit den erforderlichen Hard- und Software-Komponenten zur Verfügung.

Der Kunde verpflichtet sich, die XignSys mit allen für den Betrieb notwendigen Maßnahmen zu unterstützen, welche nicht im Wirkungsbereich der XignSys liegen.

Die Nutzung wird entsprechend dem vereinbarten Pay-per-User-Modell fakturiert.

XignIn Private	
Anbindung (siehe Kapitel 2)	
JS Login (embedded)	+ (Einbettung durch Kunden)
OIDC	+
SAML	€ (auf Anfrage)
User Onboarding (siehe Kapitel 3)	
via App	Abhängig von app-seitiger Umsetzung des Kunden
via XignIn-Manager	+
Remote via Remote Registration API	€
Remote via OIDC	€
Identity- und Access Management (siehe Kapitel 4)	
Ein-Faktor-Authentifizierung	+
Zwei-Faktor-Authentifizierung	+
Multi-Faktor-Authentifizierung	€
Variable Authentifzierungsfaktoren	€

Autorisierung und Rollen	+
Self-Service: Globale Administration	+
Self-Service: Organisationen	
Multiple Dienste	+
Nutzer:innen & Rechte	+
Self-Service: Dienste	
Regulierung erforderlicher Daten	+
Nutzer:innen & Rechte	+
Rollen	+
Restriktiver Zugriff	+
Verschlüsselung	+
Self-Service: Nutzer:innen	+
Remote Management (bspw. KeyCloak)	€€ (auf Anfrage)
Usability (siehe Kapitel 5)	
Ganzheitlich optimierte und konsistente User Experience	Abhängig von app-seitiger Umsetzung des Kunden
Barrierefreie App nach WCAG 2.1 Level AA+	Abhängig von app-seitiger Umsetzung des Kunden
Orts- und zeitunabhängige Authentifizierung	+
Multiple Geräte	+ (via XignIn-Manager) Via App: Abhängig von app-seitiger Umsetzung des Kunden
Nachtragen fehlender erforderlicher Datenattribute während Authentifizierung	Abhängig von app-seitiger Umsetzung des Kunden
Flexibilität und Anpassungsfähigkeit (siehe Kapitel 6)	
Standard Einstiegspunkte Authentifizierung (QR-Code, Intent/Custom URL)	+

Premium Einstiegspunkte Authentifizierung (Push, NFC, Bluetooth, WLAN, RFID, Sound)	€(€) (auf Anfrage)
XignIn-Manager als Identity Provider	+
Kundeneigener Identity Provider (via OIDC)	+
Custom Branding für Endnutzer	
Login via JS Login	+
Login via OIDC	+
App	+
E-Mails	+
Erweiterbarkeit (siehe Kapitel 7)	
Kontextbasierte Authentifizierungsfaktoren (Verhalten, Standort, Handeln)	€ (auf Anfrage)
InApp-Authentifizierung	Abhängig von app-seitiger Umsetzung des Kunden
Multiple Apps	€
KYC	€ (auf Anfrage)
Spezifische Anforderungen	€€ (auf Anfrage)
Sicherheit und Datenschutz (siehe Kapitel 8)	
Passwortlose Authentifizierung	+
Digitale Zertifikate	+
Starke Verschlüsselung	+
Nutzerdaten	+
Datentransparenz	Abhängig von app-seitiger Umsetzung des Kunden
Zertifizierungen und Prüfberichte	- (Nicht im Verantwortungsbereich der XignSys)
Produktsupport (siehe Kapitel 9)	

Sicherheits-Updates	+
Produkt-Updates/-Upgrade	€€
Störungsbeseitigung	+
Service Level & Verfügbarkeit	- (Nicht im Verantwortungsbereich der XignSys)
Support Level Bronze	+
Support Level Silber	€
Support Level Gold	€€
Zusätzliche Dienstleistungen (bspw. Consulting, Schulungen, Aufbau eines Identity Management Systems, Identity Management als Managed Service)	€(€) (auf Anfrage)

+	Leistung in der Produktvariante enthalten
-	Leistung in der Produktvariante nicht enthalten
€	Leistung gegen zusätzliches Entgelt in der Produktvariante zubuchbar

2. Anbindung

Die Anbindung der XignIn-Technologie an Kundenapplikationen kann auf unterschiedliche Art und Weise erfolgen. Das Leistungsangebot der XignSys umfasst die Einbettung des sogenannten JS Logins in Javascript-fähige Webapplikationen in Form einer Javascript-Bibliothek und die Anbindung über offene Industriestandards wie OpenID Connect und SAML.

2.1 JS Login

Beim JS Login handelt es sich um eine Javascript-Bibliothek die es Kunden ermöglicht, den Xign.Me-Login nativ in ihre Anwendungen einzubetten. Die Konfiguration erfolgt auf Dienstebene innerhalb des XignIn-Managers.

Grundsätzlich ist der JS Login für das Abrufen und Anzeigen der Einstiegspunkte zum Anstoßen eines Authentifizierungsvorgangs gegenüber des jeweiligen Dienstes verantwortlich. Im Anschluss an eine erfolgreiche Authentifizierung findet eine Weiterleitung an den konfigurierten Endpunkt statt. So wird beispielsweise der QR-Code für den Login an einem Dienst durch den JS Login vom XignIn-Manager abgerufen und für die Nutzer:innen dargestellt. Nach erfolgreicher Authentifizierung der Nutzer:in kann der weiterführende Prozess wie folgt verarbeitet werden:

- **Callback-Methode**
  Der JS Login führt eine Callback-Methode, die den AuthorizationCode enthält, (Javascript-seitig) aus. Kund:innen haben dadurch die Möglichkeit direkt per Javascript entsprechend zu reagieren (Interaktiver Modus).
- **Weiterleitung**
  Der JS Login leitet zur zuvor definierten Redirect URI inklusive des AuthorizationCodes weiter.

2.2 OpenID Connect

Das OIDC-Modul des XignIn-Managers stellt Funktionalitäten und spezifische Endpunkte für eine Anbindung über den offenen Standard OpenID Connect bereit. Alle erforderlichen Daten zur Anbindung und Konfiguration werden auf Dienstebene innerhalb des XignIn-Managers bereitgestellt. Konform zur OIDC-Spezifikation kann der Abruf wichtiger URLs und Claims zusätzlich über den „.well-known“-Endpunkt erfolgen.

Die entsprechenden signierten Nutzerdaten können nach erfolgreicher Authentifizierung der Nutzer:in mithilfe des AuthorizationCodes, der ClientID und des ClientSecrets abgerufen werden.

Optional besteht die Möglichkeit die über die TokenURL angeforderten Daten asymmetrisch oder symmetrisch zu verschlüsseln.

2.3 SAML

Das SAML-Modul des XignIn-Managers stellt Funktionalitäten und spezifische Endpunkte für eine Anbindung über den offenen Standard der Security Assertion Markup Language bereit.

In diesem Kontext unterstützt der XignIn-Manager das Browser SSO Profile mit dem HTTP-POST-, sowie das HTTP-Redirect-Binding. Für die erfolgreiche Integration müssen Metadaten zwischen dem Identity Provider (XignIn-Manager) und dem Service Provider (zu integrierende Anwendung) ausgetauscht werden.

Die Metadaten des XignIn-Managers werden über einen dedizierten Endpunkt bereitgestellt. Der Client für die zu integrierende Anwendung kann über den Upload der entsprechenden Metadaten-XML-Datei oder direkt über die Oberfläche des XignIn-Managers konfiguriert werden.

3. User Onboarding

Damit Nutzer:innen sich mithilfe Ihres persönlichen Smartphones und einer App, mit integriertem XignIn-SDK, gegenüber Diensten authentifizieren können, ist grundsätzlich eine Registrierung am XignIn-Manager erforderlich.

Diese Registrierung kann je nach Anwendungsszenario auf unterschiedlichen Wegen durchgeführt werden, setzt jedoch immer eine nicht vergebene E-Mail-Adresse (im Kontext des XignIn-Managers) und eine festzulegende PIN voraus. Nutzer:innen werden innerhalb eines XignIn-Managers global angelegt, eine erneute Registrierung einer bereits vergebenen E-Mail ist nicht möglich.

Im Anschluss an eine Registrierung muss das erstellte (Xign.Me-)Profil in einem einmaligen Aktivierungsvorgang mit der entsprechenden App auf dem persönlichen Smartphone verknüpft werden. Dazu erhalten Nutzer:innen abhängig vom Anwendungsszenario und der Umsetzung entweder eine E-Mail mit seinen Aktivierungsdaten oder kann die Aktivierung direkt über die Kundenapplikation durchführen.

Hinweis: Das „Xign.Me“ in Xign.Me-Profil wird hier geklammert, da je nach Produktvariante und Customizing die Benennung entsprechend variieren kann.

Da Nutzer:innen im Kontext eines XignIn-Managers global angelegt werden, ist eine Authentifizierung gegenüber allen öffentlichen Diensten möglich. Der Zugriff auf Dienste kann über die entsprechende Konfiguration des Access Managements reguliert werden. (Weitere Informationen unter 4.3.3.4 Restriktiver Zugriff)

3.1 Via App

Das XignIn-SDK bietet die Funktionalität der App-seitigen Registrierung. Je nach Implementierung erhalten Nutzer:innen also die Möglichkeit, sich über die Kunden- bzw. Xign.Me-App direkt zu registrieren und somit ein global gültiges (Xign.Me-)Profil zu erstellen. Die Aktivierungsdaten zur Verknüpfung des (Xign.Me-)Profils mit der entsprechenden App erhalten Nutzer:innen im Anschluss per E-Mail.

3.2 Via XignIn-Manager

Über das Registrierungsformular des XignIn-Managers ist es Nutzer:innen möglich, ein global gültiges (Xign.Me-)Profil zu erstellen. Die Aktivierungsdaten zur Verknüpfung des (Xign.Me-)Profils mit der entsprechenden App erhalten Nutzer:innen im Anschluss per E-Mail.

3.3 Remote via RR API

Mithilfe der Remote Registration API (RR API) des XignIn-Managers kann die Registrierung einer Nutzer:in ausgehend von der Kundenapplikation per API-Key angestoßen werden. API-Keys werden pro Dienst ausgestellt und konfiguriert.

Die Kundenapplikation stellt eine Anfrage an den XignIn-Manager mit der entsprechenden E-Mail-Adresse und einer PIN. Die PIN kann entweder seitens der Kundenapplikation für die Nutzer:innen generiert oder aber direkt von den Nutzer:innen selbst festgelegt werden.

Im Anschluss an die erfolgreiche Registrierung erhält die Kundenapplikation vom XignIn-Manager den Aktivierungs-QR-Code. Die Nutzer:innen scannen diesen mit der entsprechenden App, bestätigt den Vorgang mit der PIN und hat somit sein (Xign.Me-)Profil mit der App verknüpft. Nach erfolgreicher Aktivierung kann die Kundenapplikation die jeweilige MappingID periodisch anfragen und das Nutzer:innen-Mapping durchführen.

3.4 Remote via OIDC

Das OIDC-Modul des XignIn-Managers bietet die Möglichkeit, die Registrierung einer Nutzer:in über OpenID Connect ausgehend von der Kundenapplikation anzustoßen. Die Nutzer:in wird in diesem Falle von der Kundenapplikation zur OIDC-Registrierungsseite des XignIn-Managers weitergeleitet.

Über die OIDC-Registrierungsseite gibt die Nutzer:in die erforderlichen Daten ein und sendet die Registrierung ab. Im Anschluss an die erfolgreiche Registrierung wird der Aktivierungs-QR-Code angezeigt. Die Nutzer:in scannt diesen mit der entsprechenden App, bestätigt den Vorgang mit der PIN und hat somit das (Xign.Me-)Profil mit der App verknüpft.

Die entsprechenden signierten Nutzerdaten können nach erfolgreicher Registrierung der Nutzer:in mithilfe des AuthorizationCodes, der ClientID und des ClientSecrets abgerufen werden.

4. Identity- und Access Management

Neben der Rolle einer Trusted Third Party, nimmt der XignIn-Manager darüber hinaus die Rolle einer Access Management Lösung ein und stellt zusätzlich Funktionalitäten einer Identity Management Lösung bereit.

4.1 Authentifizierung

Die XignIn-Technologie ermöglicht Kund:innen die Umsetzung von passwortlosen Authentifizierungslösungen basierend auf dem persönlichen Smartphone der Nutzer:in. Zusätzliche Hardware ist nicht erforderlich.

Durch die flexibel wählbare Anzahl und Art der Authentifizierungsfaktoren werden auch spezifischste Kundenanforderungen erfüllt. Zur Verfügung stehen folgende Faktoren:

- Besitz: Persönliches **Smartphone** der Nutzer:in
- Wissen: Durch Nutzer:in festgelegte **PIN**
- Biometrie: **Biometrisches Merkmal** wie etwa Fingerabdruck oder Gesicht
- Kontextbasierte Faktoren: Verhalten, Standort, Handeln (Weitere Informationen unter Kapitel 7.1)

4.1.1 Ein-Faktor-Authentifizierung

Die Umsetzung einer Ein-Faktor-Authentifizierungslösung basiert auf dem Faktor Besitz. Für eine erfolgreiche Authentifizierung ist lediglich der Besitz des persönlichen Smartphones anhand der digitalen Zertifikate und Signatur nachzuweisen.

4.1.2 Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung setzt sich aus den Faktoren Besitz und Biometrie **oder** PIN zusammen. Für eine erfolgreiche Authentifizierung ist zum einen der Besitz des persönlichen Smartphones anhand der digitalen Zertifikate und Signatur nachzuweisen, zum anderen ist eine zusätzliche Bestätigung durch das hinterlegte biometrische Merkmal **oder alternativ** der entsprechenden PIN erforderlich.

4.1.3 Multi-Faktor-Authentifizierung

Eine Multi-Faktor-Authentifizierung dient der Verifizierung von Nutzer:innen anhand einer Kombination unterschiedlicher und insbesondere unabhängiger Klassen von Authentifizierungsfaktoren.

Im Kontext der XignIn-Technologie lässt sich eine Multi-Faktor-Authentifizierung typischerweise mit der Kombination aus den Faktoren Besitz, Biometrie und Wissen realisieren. In diesem Fall wäre für eine erfolgreiche Authentifizierung zum einen der Besitz des persönlichen Smartphones anhand der digitalen Zertifikate und Signatur nachzuweisen, eine zusätzliche Bestätigung durch das hinterlegte biometrische Merkmal und die korrekte Eingabe der entsprechenden PIN erforderlich.

Auf Anfrage können durch kontextbasierte Faktoren auch weitere Kombinationen zur Umsetzung einer Multi-Faktor-Authentifizierung angeboten werden.

4.1.4 Variable Authentifizierungsfaktoren

Mithilfe des XignIn-Managers können die Authentifizierungsfaktoren flexibel gewählt und variabel miteinander kombiniert werden. Im Bezug auf die Umsetzung einer Multi-Faktor-Authentifizierung können sich dadurch die vertraglich vereinbarten Faktoren ändern und zu einer preislichen Anpassung hinsichtlich der Lizenzgebühren führen.

4.2 Self-Service

Im Kontext des Identity und Access Managements stellt der XignIn-Manager umfangreiche Konfigurationsmöglichkeiten zur Verwaltung von Organisationen und Diensten als Self-Service zur Verfügung. Auch Nutzer:innen haben die Möglichkeit selbstständig Profildaten und Geräte zu verwalten.

4.2.1 Globale Administration

Neben der Verwaltung von Organisationen und Diensten bietet der XignIn-Manager bei Bedarf auch die Möglichkeit der globalen Administration als Self-Service an. Kund:innen erhalten dadurch die vollständige Kontrolle und Zugriff auf die globalen Konfigurationsmöglichkeiten des XignIn-Managers.

Diese Option steht nur in der Produktvariante XignIn Private (Self-Hosted) zur Verfügung und erfordert eine umfangreiche Systemkenntnis hinsichtlich Funktionsweise und technischem Aufbau. Die XignSys empfiehlt die Nutzung der globalen Administrationsmöglichkeiten erst nach einer entsprechenden Schulung.

4.2.2 Organisationen

Organisationen stellen im Kontext des XignIn-Managers typischerweise ein Unternehmen bzw. eine Kommune dar. Bei entsprechender globaler Konfiguration kann in der Theorie jede Nutzer:in eine Organisation erstellen. Organisationen dienen der Verwaltung der zugeordneten Dienste, dem Rechtemanagement von Nutzer:innen auf Organisationsebene und dem Hinterlegen relevanter Unternehmensinformationen.

Grundsätzlich gilt: Eine Authentifizierung gegenüber einer Organisation ist nicht möglich. Daher muss pro kundenseitiger Anwendung innerhalb der Organisation ein Dienst angelegt werden.

4.2.2.1 Multiple Dienste

Für die Inbetriebnahme der Authentifizierungslösung in einer kundenseitigen Anwendung muss auf der Seite des XignIn-Managers pro Anwendung ein Dienst angelegt und entsprechend konfiguriert werden. Dienste sind immer einer Organisation zugeordnet – eine technische Limitierung hinsichtlich der Anzahl an Diensten pro Organisation existiert nicht.

4.2.2.2 Nutzer:innen und Rechte

Nutzer:innen können einer Organisation ausschließlich per Einladung hinzugefügt werden. Über das Rechtemanagement besteht die Möglichkeit Nutzer:innen auf Organisationsebene spezifische Rechte zuzuweisen. Das Rechtemanagement umfasst unter anderem:

- Hinzufügen und Entfernen von Nutzer:innen der Organisation
- Bearbeiten und Löschen der Organisation
- Anlegen von Diensten innerhalb der Organisation

4.2.3 Dienste

Dienste stellen im Kontext des XignIn-Managers typischerweise eine Kundenapplikation dar und bieten umfangreiche Konfigurationsmöglichkeiten. Neben dem Rechtemanagement von Nutzer:innen auf Dienstebene und der Zuweisung frei definierbarer Rollen können die zur Authentifizierung erforderlichen Daten flexibel angepasst und der globale Zugriff auf den Dienst beschränkt werden.

4.2.3.1 Erforderliche Daten

Für die erfolgreiche Authentifizierung gegenüber einem Dienst werden von Nutzer:innen gewissen Daten angefordert. Kund:innen können über die Konfigurationseinstellungen eines Dienstes definieren, welche Daten erforderlich sind. Zur Auswahl stehen zahlreiche Datenattribute, die flexibel kombiniert werden können. Nutzer:innen haben je nach Produktvariante und App-seitiger Umsetzung die Möglichkeit, nicht vorhandene erforderliche Datenattribute während eines Authentifizierungsvorgangs nachzutragen.

4.2.3.2 Nutzer:innen und Rechte

Auf Dienstebene stellt der XignIn-Manager Kund:innen Funktionalitäten zur Verwaltung von Nutzer:innen und deren Rechte bereit. Wird für die Nutzung des Dienstes beispielsweise eine explizite Einladung vorausgesetzt, so können Kund:innen Nutzer:innen per Einladung hinzufügen. Über das Rechtemanagement besteht die Möglichkeit Nutzer:innen auf Dienstebene spezifische Rechte zuzuweisen. Das Rechtemanagement umfasst unter anderem:

- Hinzufügen und Entfernen von Nutzer:innen des Dienstes
- Erstellen, Bearbeiten und Löschen von Rollen
- Konfiguration des Dienstes durch Nutzer:in

- Bearbeiten und Löschen des Dienstes
- Anlegen von Diensten innerhalb der Organisation

4.2.3.3 Rollen

Pro Dienst sind spezifische Rollen definierbar. Dies ermöglicht die rollenbasierte Authentifizierung gegenüber Diensten. Sollte es erforderlich sein, höherwertige und sicherheitskritische Rollen stärker abzusichern, so haben Kund:innen grundsätzlich die Möglichkeit, für jede Rolle unterschiedliche Authentifizierungsfaktoren festzulegen.

4.2.3.4 Restriktiver Zugriff

Da Nutzer:innen im Kontext eines XignIn-Managers im Zuge der Registrierung global angelegt werden, ist eine Authentifizierung gegenüber allen öffentlichen Diensten möglich. Der Zugriff auf Dienste kann über die entsprechende Konfiguration des Access Managements reguliert werden. Pro Dienst stehen als Zugriffsbeschränkung folgende Optionen zur Verfügung:

- **Mitgliedschaft in Organisation erforderlich**
  Nutzer:in kann Dienst nur dann nutzen, wenn eine Mitgliedschaft in der übergeordneten Organisation vorliegt
  (Hier ist zu beachten: Nutzer:innen eines Dienstes müssen nicht zwangsläufig auch Mitglied der übergeordneten Organisation sein.)
- **Einladung erforderlich**
  Nutzer:in kann Dienst nur dann nutzen, wenn eine explizite Einladung zum Dienst erfolgt ist und die Einladung nutzer:innenseitig akzeptiert wurde

4.2.3.5 Verschlüsselung

Nach erfolgreicher Authentifizierung sind die jeweiligen relevanten Nutzerinformationen über die TokenURL abrufbar. Die Integrität dieser Daten wird durch Überprüfen der digitalen Signatur verifiziert. Zusätzlich haben Kund:innen die Möglichkeit, die Abfrage der Nutzerinformationen symmetrisch oder asymmetrisch (EC oder RSA) zu verschlüsseln.

4.2.4 Nutzer:innen

Die Self-Service-Funktionalität des XignIn-Managers ermöglicht es Nutzer:innen, ihr (Xign.Me-)Profil vollumfänglich zu verwalten. Folgende Funktionen stehen Nutzer:innen unter anderem zur Verfügung:

- Anpassen der persönlichen Profildaten
- Einsicht und Verwaltung aller genutzten Dienste
- Einsicht und Verwaltung aller Organisationsmitgliedschaften
- Einsicht und Verwaltung aller Aktivierungen

4.3 Remote Management

Mithilfe der Remote Management API erhalten Kund:innen die Möglichkeit, ausgehend von der kundeneigenen Applikation über einen API Key auf die Funktionalitäten des Identity und Access Management Systems (IAM) zurückzugreifen. Als IAM können hierfür beispielsweise die Open-Source-Lösung KeyCloak oder die Identitätsplattform ForgeRock eingesetzt werden.

5. Usability

Das Thema Usability stellt eine zentrale Säule der XignIn-Technologie dar. Für Nutzer:innen und Kund:innen wird ein herausragendes Nutzererlebnis geschaffen, ohne Einbußen in puncto Sicherheit in Kauf nehmen zu müssen. Mit dieser einzigartigen Kombination bietet die XignSys ein nachhaltiges und interoperables Leistungspaket für unterschiedlichste Anwendungsfälle, das auf einer einfachen, komfortablen und konsistenten Usability basiert.

5.1 User Experience

Im Kontext einer Authentifizierung trägt der Verzicht auf Passwörter maßgeblich zur Verbesserung des Nutzer:innenerlebnisses bei. Die intuitive passwortlose Authentifizierung mittels der XignIn-Technologie befreit Nutzer:innen von Passwortmüdigkeit, bietet ein frustfreies Login-Erlebnis und steigert nachweislich die Produktivität.

Darüber hinaus sind alle Komponenten der XignIn-Technologie mit großer Sorgfalt hinsichtlich Gestaltung, Terminologie und Nutzer:innenführung konsistent aufeinander abgestimmt, wodurch sich ein ganzheitlich optimiertes Nutzer:innenerlebnis ergibt.

Basierend auf dem regelmäßigen Austausch mit Nutzer:innen über Plattformen wie XignSys Ideas oder ähnlichen digitalen Kanälen, sowie Testveranstaltungen vor Ort, werden Prozesse und Nutzer:innenführung stets nutzer:innenorientiert überprüft und optimiert. Durch die vollständige Datentransparenz in jeglichen Prozessen und die vielfältigen Möglichkeiten zur Selbstverwaltung des persönlichen (Xign.Me-)Profils wird die nutzer:innenseitige Akzeptanz erhöht und das Vertrauen gestärkt.

5.2 Barrierefreiheit

Die Xign.Me-App gewährleistet eine gute Zugänglichkeit für Alle nach dem internationalen Standard für Web- und Mobilanwendungen des W3-Consortiums WCAG2.1. Im Rahmen dieser Richtlinie erfüllt die Xign.Me-App neben den Mindestanforderungen (Level A) auch die erweiterten Anforderungen (Level AA), sowie in diesem Kontext alle sinnvollen zusätzlichen Anforderungen (Level AA+).

Dadurch wird eine effektive Barrierefreiheit sowie gute Zugänglichkeit für Alle sichergestellt und auch die entsprechenden Anforderungen an Software im öffentlichen Bereich abgedeckt.

5.3 Orts- und Zeitunabhängigkeit

Die einfache und sichere Authentifizierung mithilfe der XignIn-Technologie erfolgt orts- und zeitunabhängig über das persönliche Smartphone der Nutzer:innen.

5.4 Multiple Geräte

Die XignIn-Technologie unterstützt die Nutzung eines (Xign.Me-)Profils auf multiplen Geräten. Pro Gerät ist jeweils eine sogenannte Aktivierung erforderlich. Nutzer:innen können beliebig viele Aktivierungen ihrem (Xign.Me-)Profil hinzufügen und diese über den XignIn-Manager verwalten.

Abhängig von der Produktvariante und der entsprechenden App-seitigen Umsetzung stehen prinzipiell drei verschiedene Szenarien zur Verfügung, wie Nutzer:innen Ihrem (Xign.Me-)Profil eine Aktivierung hinzufügen können:

- Hinzufügen einer Aktivierung über den XignIn-Manager (unabhängig von App-seitiger Umsetzung)
- Hinzufügen einer Aktivierung über die Einstellungen einer bereits aktivierten App (abhängig von App-seitiger Umsetzung)
- Hinzufügen einer Aktivierung während des Aktivierungsvorgangs einer nicht aktivierten App (abhängig von App-seitiger Umsetzung)

5.5 Nachtragen fehlender Datenattribute

Für die Authentifizierung gegenüber einem Dienst sind üblicherweise gewisse Datenattribute erforderlich. Mithilfe der Access Management Funktionalität des XignIn-Managers können diese erforderlichen Datenattribute pro Dienst variabel definiert werden. Nutzer:innen haben je nach App-seitiger Umsetzung die Möglichkeit, fehlende erforderliche Datenattribute während eines Authentifizierungsvorgangs direkt in der entsprechenden App nachzutragen. Der Vorgang wird nicht unterbrochen und kann im Anschluss fortgeführt werden.

6. Flexibilität und Anpassungsfähigkeit

Die XignIn-Technologie stellt eine sehr flexible Authentifizierungslösung dar, die auch speziellen Kundenanforderungen gerecht wird. Die Lösung ist hinsichtlich unterschiedlichster Kriterien und Anforderungen anpassbar und kann dadurch in nahezu allen denkbaren Anwendungsbereichen eingesetzt werden.

6.1 Einstiegspunkte

Kund:innen haben die Möglichkeit je nach Anwendungsbereich und -szenario den Einstiegspunkt zum Anstoßen eines Authentifizierungsvorgangs frei zu wählen. Zur Auswahl stehen unterschiedlichste Einstiegspunkte, die ein sehr breites Spektrum für die Umsetzung von digitalen und realen Anwendungsfällen abdecken.

6.1.1 Standard

Standardmäßig umfasst der Leistungsumfang der XignIn-Technologie die folgenden typischen Einstiegspunkte:

- **QR-Code**
  Um eine Authentifizierung via QR-Code anzustoßen, muss dieser lediglich mithilfe des persönlichen Smartphones und einer App, mit integriertem XignIn-SDK, gescannt werden. Der Vorgang wird innerhalb der App nach erfolgreicher Bestätigung der entsprechenden Faktoren durch die Nutzer:in binnen weniger Sekunden abgeschlossen. Typischerweise kommt der QR-Code vor allem bei Anwendungsfällen zum Einsatz, die eine Authentifizierung an einem Zweitgerät erfordern, beispielsweise Desktop-Anwendungen, Ladesäulen oder auch Packstationen.
  (Grundsätzlich können die QR-Codes der XignSys auch mit jeder beliebigen Systemkamera des Smartphones gescannt werden. Befindet sich die entsprechende zu öffnende App auf dem Smartphone, so wird diese gestartet und der Vorgang kann nutzer:innenseitig abgeschlossen werden. Ist die erforderliche App nicht auf dem Smartphone installiert, gelangen Nutzer:innen über eine Landingpage zur App im jeweiligen App Store.)
- **Mobile Links** (Android: Intent, iOS: Custom URL)
  Die sogenannten Mobile Links dienen vor allem der Authentifizierung auf einem mobilen Gerät, beispielsweise dem Smartphone. Verpackt als Buttons ermöglichen Sie das Anstoßen einer Authentifizierung, indem die entsprechende App, mit integriertem XignIn-SDK, auf demselben Gerät geöffnet wird. Der Vorgang wird innerhalb der App nach erfolgreicher Bestätigung der entsprechenden Faktoren durch die Nutzer:in binnen weniger Sekunden abgeschlossen.

6.1.2 Premium

Die Interoperabilität der XignIn-Technologie zeichnet sich unter anderem dadurch aus, dass auch für spezifische Kundenanforderungen und Anwendungsfälle eine Authentifizierungslösung angeboten und umgesetzt werden kann. Hierfür stehen auf Anfrage eine Reihe weiterer zusätzlicher Einstiegspunkte zur Verfügung:

- PUSH
- NFC
- Bluetooth
- WLAN
- RFID
- Sound

Sie benötigen eine Authentifizierungslösung basierend auf einem weiteren, hier nicht aufgeführten, Einstiegspunkt? Die XignIn-Technologie lässt sich für jeden denkbaren Anwendungsfall integrieren - nehmen Sie gerne mit uns Kontakt auf!

6.2 Identity Provider (IdP)

Im Kontext der Authentifizierung können Kund:innen frei entscheiden, welcher Dienst als Identity Provider eingesetzt werden soll. Grundsätzlich steht hier zum einen der XignIn-Manager zur Verfügung oder alternativ ein kundeneigener Dienst.

Die Anbindung eines kundeneigenen Identity Providers erfolgt idealerweise über den offenen Standard OpenID Connect. Sollte diese Anbindung nicht möglich sein, ein kundeneigener Identity Provider jedoch erforderlich, so kann auf Anfrage eine entsprechende Lösung gemeinsam eruiert werden.

6.3 Custom Branding für Endnutzer

Je nach Produktvariante haben Kund:innen die Möglichkeit, die für die Nutzer:innen sichtbaren Anwendungsoberflächen hinsichtlich des Brandings anzupassen und somit eine White Label Authentifizierungslösung umzusetzen. Dies macht vor allem im Kontext der Produktvariante XignIn Private Sinn.

Prinzipiell übernehmen wir auf Anfrage für Sie die Anpassungen und setzen Ihr Custom Branding gegen ein entsprechendes Entgelt um.

6.3.1 Login via JS Login

Die Oberfläche des Logins via JS Login umfasst die Ansicht des QR-Codes sowie der Mobile Links, im Falle einer Authentifizierung auf einem mobilen Gerät. Hier besteht die Möglichkeit das Branding spezifisch pro Dienst zu konfigurieren. Folgende Konfigurationsmöglichkeiten stehen grundsätzlich zur Verfügung:

- **Farben**
  Die Farben des grafischen Rahmens der QR-Code Ansicht und der Button für den mobilen Login können entsprechend dem kundenspezifischen Corporate Design angepasst werden.
- **App- und Profilbezeichnung (Naming)**
  Je nach Produktvariante und Umsetzung ist es nötig und möglich sowohl die Benennung der App, als auch die Bezeichnung des Profils festzulegen.
- **Herstellerverweis**
  Der XignSys Herstellerverweis kann aktiviert und deaktiviert werden. Das Deaktivieren darf nur auf Basis einer entpsrechenden vertraglichen Vereinbarung erfolgen.

6.3.2 Login via OIDC

Die Oberfläche des Logins via OIDC umfasst die Ansicht des QR-Codes sowie der Mobile Links, im Falle einer Authentifizierung auf einem mobilen Gerät. Anders als beim Login via JS Login ist die Login Seite via OIDC global im Kontext des jeweiligen XignIn-Managers gültig. Ein spezifisches Branding ist demnach nur für die Produktvariante XignIn Private umsetzbar. Folgende Konfigurationsmöglichkeiten stehen grundsätzlich zur Verfügung:

- **Farben**
  Die Farben des grafischen Rahmens der QR-Code Ansicht und der Button für den mobilen Login können entsprechend dem kundenspezifischen Corporate Design angepasst werden.
- **App- und Profilbezeichnung (Naming)**
  Je nach Produktvariante und Umsetzung ist es nötig und möglich sowohl die Benennung der App, als auch die Bezeichnung des Profils festzulegen.
- **Herstellerverweis**
  Der XignSys Herstellerverweis kann aktiviert und deaktiviert werden. Das Deaktivieren darf nur auf Basis einer entpsrechenden vertraglichen Vereinbarung erfolgen.

6.3.3 App

Die Produktvarianten XignIn as a Service und XignIn Private ermöglichen es Kund:innen, eine kundeneigene App mit integriertem XignIn-SDK als Authentifizierungs-Tool zu verwenden. Hinsichtlich der Oberflächengestaltung und der App-Texte gibt es keine Einschränkungen.

Bei der Umsetzung bestimmter Prozesse, wie bspw. Aktivierung und Authentifizierung, müssen die vorgesehenen Abläufe und Logiken entsprechend der Vorgaben aus den Dokumentationen berücksichtigt werden. Bei weiteren Fragen leistet die XignSys natürlich den entsprechenden Support.

6.3.4 E-Mails

Im Zuge gewisser Aktionen und Vorgänge werden Benachrichtigungen und Informationen per E-Mail an Nutzer:innen versendet. Beispielsweise erhalten

Nutzer:innen nach erfolgreicher Registrierung eine E-Mail mit den persönlichen Aktivierungsdaten oder werden über eine Einladung zu einer Organisation bzw. einem Dienst informiert.

Alle E-Mail Templates sind durchweg responsive und für die verschiedenen Endgeräte optimiert. Die XignSys testet und überprüft zudem stets die Kompatibilität der Templates mit allen relevanten und gängigen E-Mail Clients am Markt.

In der Produktvariante XignIn Private sind diese E-Mails hinsichtlich der Gestaltung vollständig anpassbar.

7. Erweiterbarkeit

Die XignIn-Technologie ist modular aufgebaut und kann bei Bedarf je nach Anwendungsfall und Kundenanforderung um ergänzende Funktionen und Features erweitert werden.

7.1 Kontextbasierte Faktoren

Neben den Standard Faktoren Besitz des Geräts, PIN und Biometrie sind für die Umsetzung einer Multi-Faktor-Authentifizierungslösung auf Basis der XignIn-Technologie auch weitere Faktoren denkbar. Kontextbasierte Faktoren beziehen die Eigenschaften Verhalten, Standort und Handeln dynamisch im jeweiligen Kontext mit ein. Generell sollten kontextbasierte Faktoren immer nur in Kombination mit nicht-kontextbasierten Faktoren verwendet werden.

7.2 InApp-Authentifizierung

In kundeneigenen Apps stehen Nutzer:innen oftmals InApp-Services zur Verfügung, für deren Nutzung vorab eine Authentifizierung nötig ist. Das XignIn-SDK kann mit dem Feature der InApp-Authentifizierung die Funktionalität bereitstellen, InApp-Services entsprechend abzusichern. Die Authentifizierung erfolgt medienbruchfrei direkt in der jeweiligen App.

7.3 Multiple Apps

Die XignIn-Technologie unterstützt die Nutzung eines (Xign.Me-)Profils für multiple Apps. Pro App ist jeweils eine sogenannte Aktivierung erforderlich. Nutzer:innen können beliebig viele Aktivierungen ihrem (Xign.Me-)Profil hinzufügen und diese über den XignIn-Manager verwalten.

Abhängig von der Produktvariante und der entsprechenden App-seitigen Umsetzung stehen prinzipiell drei verschiedene Szenarien zur Verfügung, wie Nutzer:innen Ihrem (Xign.Me-)Profil eine Aktivierung hinzufügen können:

- Hinzufügen einer Aktivierung über den XignIn-Manager (unabhängig von App-seitiger Umsetzung)
- Hinzufügen einer Aktivierung über die Einstellungen einer bereits aktivierten App (abhängig von App-seitiger Umsetzung)
- Hinzufügen einer Aktivierung während des Aktivierungsvorgangs einer nicht aktivierten App (abhängig von App-seitiger Umsetzung)

7.4 Know your Customer (KYC)

Über Technologiepartner kann die XignIn-Technologie um Legitimationsprüfungen in Form von Erstidentifikationsverfahren erweitert werden.

Je nach Anwendungsfall und Kundenanforderung würden beispielsweise innerhalb des App-seitigen Registrierungsvorgangs die entsprechenden KYC-Verfahren integriert. Die qualifizierte Datenerfassung erfolgt bei Verfahren wie etwa Video-Ident und Auto-Ident automatisch und erfordert keine nutzerseitige Eingabe.

7.5 Spezifische Anforderungen

Die XignIn-Technologie ist äußerst flexibel und auch für sehr spezifische Anforderungen anpassbar und erweiterbar. Durch die sehr gute Interoperabilität lässt sich die Authentifizierungslösung der XignSys überall integrieren und eignet sich daher auch bestens für physische Anwendungsfälle aus der realen Welt.

Über Technologiepartner wären beispielsweise digitale Türschlösser mit integrierter XignIn-Technologie realisierbar, die ein Öffnen der Tür per Smartphone und einer entsprechenden App, mit integriertem XignIn-SDK, erlaubt.

Kommen Sie für alle weiteren spezifischen Anforderungen gerne auf uns zu.

8. Sicherheit und Datenschutz

Die IT-Sicherheit und der Schutz personenbezogener Daten nehmen für die XignSys einen besonders hohen Stellenwert ein und sind fest im Leitbild des Unternehmens verankert. Durch die Maßnahmen der IT-Sicherheit werden die Vertraulichkeit, Integrität und Verfügbarkeit der XignIn-Technologie gewährleistet. Der Datenschutz hingegen stärkt und wahrt das Recht unserer Nutzer:innen auf informelle Selbstbestimmung.

Konform zur neuen Datenschutz-Grundverordnung der Europäischen Kommission hat die XignSys einen Datenschutzbeauftragten bestellt. Der Datenschutzbeauftragte wird nicht nur von einem Team aus qualifizierten Mitarbeiterinnen und Mitarbeitern unterstützt, sondern auch von renommierten wissenschaftlichen Einrichtungen. Hinsichtlich Datensicherheit arbeitet das Datenschutz-Team eng mit dem IT-Sicherheits-Team der XignSys zusammen.

8.1 Passwortlose Authentifizierung

Trotz schwerwiegender Sicherheitsrisiken und hohen ökonomischen Nachteilen sind Passwörter traditionell immer noch stark verbreitet. Leidtragende sind nicht nur Unternehmen und Kommunen, sondern auch Endnutzer:innen.

Die XignIn-Technologie basiert auf digitalen Zertifikaten und Signaturen, sowie modernsten kryptografischen Verfahren und ermöglicht so die Umsetzung sicherer passwortloser (Multi-Faktor-) Authentifizierungslösungen für jeden denkbaren Anwendungsfall.

Neben den äußerst positiven Auswirkungen auf das Nutzer:innenerlebnis, zeichnen sich auch entscheidende Vorteile für Unternehmen und Kommunen durch den Verzicht auf Passwörter ab:

- Wirksamer Schutz gegen Cyber-Angriffe
- Reduzierung des Kosten- und Zeitaufwands
- Steigerung der Nutzer:innenproduktivität im geschäftlichen Umfeld

8.2 Digitale Zertifikate und Signaturen

Die XignIn-Technologie basiert auf digitalen Zertifikaten und Signaturen, sowie modernsten kryptografischen Verfahren und löst damit herkömmliche, sicherheitskritische Authentifizierungsmethoden wie etwa Nutzername/Passwort, Einmal-TANs und kostspielige Hardware (Tokens/Schlüsselkarten) nachhaltig ab.

Im Zuge der Aktivierung des persönlichen Smartphones werden kryptographische Schlüssel auf dem Smartphone-eigenen Hardware-Sicherheitsmodul (HSM) erzeugt. Hierbei handelt es sich auf Android-Geräten um den sogenannten Hardware Backed Keystore und um die Secure Enclave bei iOS-Geräten. Der Austausch der entsprechenden öffentlichen Schlüssel mit dem XignIn-Manager findet ebenfalls während der Aktivierung statt.

Mithilfe dieser Schlüssel und dem eingesetzten Public Key Infrastructure Verfahren erfolgt die jeweilige Nutzer:innen-Authentifizierung, die durch die Kombination der Zertifikate ein Höchstmaß an Sicherheit gewährleistet.

8.3 Starke Verschlüsselung

Hinsichtlich kryptografischer Verfahren setzt die XignIn-Technologie auf die höchsten Sicherheitsstandards und den aktuellen Stand der Technik. Hierbei werden stets die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) berücksichtigt. Kund:innen können jederzeit flexibel mithilfe der entsprechenden Konfiguration eine Anpassung des anzuwendenden Verfahrens vornehmen.

8.4 Nutzerdaten

Die XignSys stellt Nutzer:innen und den Schutz ihrer Daten, sowie ihre Hoheit darüber in den Mittelpunkt. Jede Person hat ein Recht darauf, dass ihre Daten geschützt sind und sie selbst souverän entscheiden darf, wo und wie ihre Daten genutzt werden. Deshalb haben und behalten Nutzer:innen der XignIn-Technologie DSGVO-konform die volle Kontrolle über Ihre persönlichen Daten und können diese auch selbst über die Oberfläche des XignIn-Managers verwalten.

8.5 Datentransparenz

Eine weitere wichtige Rolle in der nutzer:innenorientierten Umsetzung des Datenschutzes im Kontext der XignIn-Technologie nimmt die Datentransparenz ein. Nutzer:innen haben jederzeit die vollständige Transparenz hinsichtlich der Verwendung ihrer Daten im Zuge einer Authentifizierung.

Bei jedem Vorgang erhalten Nutzer:innen eine Auflistung aller vom jeweiligen Dienst angeforderter Daten. Nur durch die explizite nutzer:innenseitige Zustimmung erfolgt im Anschluss an den erfolgreichen Authentifizierungsvorgang die Freigabe.

Je nach Produktvariante und App-seitiger Umsetzung sind alle wichtigen Informationen bezüglich vergangener Authentifizierungsvorgänge inklusive der angeforderten Daten über die Historie innerhalb der App einsehbar.

8.6 Zertifizierungen und Prüfberichte

Prüfbericht BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterzog die XignIn-Technologie einer ausführlichen Prüfung nach TR-03107-1. Anhand dieser technischen Richtlinie werden Verfahren zu elektronischen Identitäten und Vertrauensdiensten für verschiedene Prozesse des E-Governments bewertet und Vertrauensniveaus zugeordnet. Das BSI bestätigt die Eignung der XignIn-Technologie, bei entsprechender Konfiguration, als Authentisierungsmittel auf substantiellem Vertrauensniveau.

Penetrationstests

Um Sicherheitsvorfälle zu vermeiden und nachhaltig die IT-Sicherheit der XignIn-Technologie durch Dritte zu bestätigen, ergreift die XignSys präventive Maßnahmen. Die XignIn-Technologie wird von unabhängigen externen IT-Sicherheitsunternehmen durch umfangreiche Penetrationstests in regelmäßigen Abständen auf potentielle Schwachstellen überprüft.

9. Produktsupport

Die XignSys bietet für alle Produktvarianten (Xign.Me aaS, XignIn aaS und XignIn Private) kontinuierlich Sicherheits-Updates, Produkt-Updates bzw. Upgrades, kurzfristige Störungsbeseitigung sowie den gewünschten Kund:innen-Support an.

9.1 Sicherheits-Updates

Sicherheit hat für die XignSys oberste Priorität. Nach Feststellung eines notwendigen Sicherheits-Updates wird ein entsprechender Patch so schnell wie möglich zur Verfügung gestellt. Bei der Produktvariante XignIn Private erfordert ein zeitnahes Sicherheits-Update den notwendigen kundenseitigen Support und Zugriff auf das System.

9.2 Produkt-Updates /-Upgrades

Es ist unser ständiges Bestreben, unser Produkt nicht nur funktionsfähig, sondern auf dem neuesten Stand der Technik und so fortschrittlich wie möglich zu halten. Daher werden wir kontinuierlich Produkt-Updates bzw. Upgrades durchführen.

Diese Neuerungen fokussieren sich auf folgende Bereiche:

- Sicherheits-Updates
- Kontinuierliche Produkt-Updates und Produkt-Upgrades (funktionale Verbesserungen sowie Anpassungen der Standard-Software als durchgängig fortlaufender und notwendiger Prozess):
    - Bei Erweiterung, Änderung oder Wegfall von Eigenschaften der Smartphone-Betriebssysteme durch die Hersteller Google und Apple
    - Bei Neuerscheinung von Smartphone-Modellen
    - Abwärtskompatibilität von neuen Software-Versionen zu alten Smartphone-Modellen
    - Bei Änderung oder Erneuerung von kryptografischen Algorithmen aufgrund von Sicherheitsvorfällen oder zeitlichen Entwicklungen
    - Bei Anpassungen, die durch Anmerkungen und Anregungen der Nutzer:innen entstehen (kontinuierliche Updates der Benutzerfreundlichkeit)
- Neue Produktfeatures, die den bisherigen Leistungsumfang (optional) ergänzen

Der Update- bzw. Upgrade-Prozess variiert je nach gewählter Produktvariante:

- **Xign.Me as a Service**
  Produktupdates / - upgrades erfolgen automatisch. Die App Xign.Me und der XignIn-Manager werden kontinuierlich mit Updates und ggf. Upgrades versorgt

- **XignIn as a Service**
  Produktupdates / - upgrades erfolgen beim XignIn-Manager automatisch. Es muss aber sichergestellt werden, dass die Kompatibilität zwischen dem XignIn-Manager und der Kunden-App (die das XignIn-SDK integriert hat) jederzeit bestehen bleibt. Daher muss auch die Kund:innenseite dafür Sorge tragen, dass jederzeit die neueste SDK-Version genutzt wird und alle für den einwandfreien Betrieb notwendigen Features ordnungsgemäß implementiert werden. Die XignSys verpflichtet sich hierbei, sämtliche Informationen zu kommenden Updates mindestens 2 Wochen vor Release zur Verfügung zu stellen.
- **XignIn Private**
  Die Kund:in erwirbt jeweils einen funktionierenden Versionsstand des XignIn-Managers, des XignIn-SDKs und ggf. der Xign.Me App. Produktupdates oder-upgrades können danach gegen Bezahlung beauftragt und umgesetzt werden.

9.3 Service Level

Die jährliche Verfügbarkeit (Kalenderjahr) wird für das jeweilige Jahr berechnet als die maximal verfügbaren Minuten minus Ausfallzeit, geteilt durch die maximal verfügbaren Minuten im jeweiligen Jahr. Die maximal verfügbaren Minuten entsprechen der Gesamtzahl der Minuten im entsprechenden Jahr, in denen ein Vertragsverhältnis zwischen XignSys und der Kund:in besteht. Die Ausfallzeit ist die Gesamtzahl der Minuten im entsprechenden Jahr, in der die XignSys-Instanz der Kund:innen nicht verfügbar war und in der ein Vertragsverhältnis zwischen XignSys und der Kund:in bestand. Die Zeiten der genutzten Wartungsfenster fließen nicht in die Berechnung der Ausfallzeit ein.

Die Leistungen der SaaS-Plattform stehen mit einer mittleren Verfügbarkeit von 99,5 % im Jahresdurchschnitt zur Verfügung. Zeiten, in der Wartungsfenster von XignSys genutzt werden, fließen nicht in die Berechnung der Verfügbarkeit ein. Wartungen und Updates werden ausschließlich in der Zeit von Mittwochabend nach 20 Uhr bis Donnerstagmorgen 6 Uhr durchgeführt.

9.4 Störungsbeseitigung

Ein einwandfreier Betrieb der Lösungen ist der Anspruch der XignSys. Sollte es dennoch einmal zu Störungen kommen, ist es unser Ziel, diese Bugs oder Probleme so kurzfristig und kundenfreundlich wie möglich zu klären. Basis hierfür sind die individuell vereinbarten Supportlevel.

9.5 Kundensupport

Je nach Kundenbedarf werden 3 unterschiedliche Level des Supports – definiert auf Basis von Service-, Reaktions- und Wiederherstellungszeiten (Gold, Silber und Bronze) angeboten, die in der Folge näher beschrieben werden. Der gewünschte Supportlevel wird bei der Beauftragung des Auftragnehmers festgelegt.

Support-Varianten	Art der Störung	Servicezeiten				Reaktionszeit		Wiederherstellungszeit*	
		Servicestunden pro Tag	Zeitraum pro Tag	Tage		Stunden	Tage	Stunden	Tage
Bronze	Betriebsverhindernde Störung	8	9-17 Uhr	5	Mo - Fr	4	0,5	24	3
	Betriebsbehindernde Störung	8	9-17 Uhr	5	Mo - Fr	8	1	80	10
	Leichte Störung	8	9-17 Uhr	5	Mo - Fr	16	2	160	15
Silber	Betriebsverhindernde Störung	12	8-20 Uhr	5	Mo - Fr	4	0,3	24	2,0
	Betriebsbehindernde Störung	12	8-20 Uhr	5	Mo - Fr	8	0,7	80	6,7
	Leichte Störung	12	8-20 Uhr	5	Mo - Fr	16	1,3	160	13,3
Gold	Betriebsverhindernde Störung	24	0-24 Uhr	7	Mo - So	4	0,2	24	1,0
	Betriebsbehindernde Störung	24	0-24 Uhr	7	Mo - So	8	0,3	80	3,3
	Leichte Störung	24	0-24 Uhr	7	Mo - So	16	0,7	160	6,7

- Reaktions- und Wiederherstellungszeiten beginnen ausschließlich mit dem Zugang der Störungsmeldung während der vereinbarten Servicezeiten und laufen ausschließlich während der vereinbarten Servicezeiten.
- Die Wiederherstellungszeit startet erst, sobald wir alle relevanten Informationen zu einer entsprechenden Störung erhalten haben. Diese werden innerhalb des Vertrages definiert
- Störungen können telefonisch, per E-Mail oder über ein Ticketsystem gemeldet werden. Es gelten folgende Kontaktdaten
- Name/Firma: XignSys GmbH Organisationseinheit/Abteilung: Customer Service Postanschrift: Bochumer Straße 110, 45886 Gelsenkirchen Telefon: +49209 883 044 0
- E-Mail: **support@xignsys.com** Web-Adresse: www.xignsys.com

9.6 Zusätzliche Dienstleistungen

In Ergänzung zu den oben beschriebenen Software-Lösungen bieten wir als XignSys folgende zusätzliche Lösungen (Software & Dienstleistungen) an:

- Authentifizierung basierend auf FIDO2
- Beratung / Workshop für die Definition und Umsetzung von (Smart-City) Use Cases im Kontext der Authentifizierungslösung XignIn.
- Beratung und Umsetzung der Integration des Servicekontos in eine Anwendung (z.B. App, einzelne Dienste, Portale, Websites etc.).
- Schnittstellen Programmierung für die Nutzung des ServiceKontos
- Konzeption & Aufbau eines Identity- und Access-Management-Systems
- Aufbau, Betrieb, Weiterentwicklung einer Smart City Plattform zur Authentifizierung von Bürger:innen, Daten und Bürgerinformationen.