DEUTSCH

# CONNECTING IDEAS THROUGH OPEN SOURCE

IDENTITY & ACCESS MANAGEMENT.
FEDERATED INFRASTRUCTURES.
OPEN SOURCE.

DAASI International

Diese Broschüre

# INHALT

## ÜBER DAASI INTERNATIONAL


Vorwort des Gründers 4
Vorwort der Geschäftsführer 5
Warum Open Source? 6
Projektmanagement 7


## IDENTITY & ACCESS MANAGEMENT


Expertin für IAM 8
IdM-Lösungen 10
didmos 12
SSO-Technologien 14
Leistungen 16
Erfolgsgeschichten 18


## INFRASTRUKTUR


DH-Infrastruktur 22
User-zentrtierte Identität 24


## FORSCHUNG


Foschungsbeteiligung 26

Peter Gietz

# VORWORT DES GRÜNDERS

Die DAASI International steht für Professionalität, Engagement, Nachhaltigkeit, Fairness und digitale Souveränität. Diese Werte sind tief in unserer Unternehmensphilosophie verankert und mit ein Grund dafür, warum wir zu den führenden Open-Source-Anbietern im Bereich Identity & Access Management (IAM) gehören.

Der Ursprung der DAASI International liegt in der Forschung. Als Spin-off eines Forschungsprojektes des Deutschen Forschungsnetzes (DFN) an der Universität Tübingen setzten wir uns das Ziel, einem engagierten Team interessante und abwechslungsreiche Arbeitsplätze zu schaffen und innovative Technologien zu fördern.

Heute verfügen wir über eine europaweit gefragte Expertise für föderiertes Identity & Access Management. Wir helfen Organisationen, ihre IT-Infrastruktur mit moderner Technologie auf Open-Source-Grundlage effizienter und sicherer zu machen und sorgen für eine verlässliche und intuitiv bedienbare Infrastruktur. Wir erleichtern damit die tägliche Arbeit vieler Nutzer*innen trotz zunehmender Komplexität der IT-Landschaft und erhöhen die IT-Sicherheit. Da IAM-Technologien und -Methoden ebenfalls in virtuellen Forschungsumgebungen benötigt werden, bringen wir unser Fachwissen auch in Forschungsinfrastrukturen, etwa im Rahmen der Nationalen Forschungsdateninitiative (NFDI), ein.

Unsere langjährige Erfahrung, die Förderung von Open-Source-Technologien, offenen Standards und Datenschutz im Sinne digitaler Souveränität sowie unser Engagement in der Forschung zeichnen uns aus. Wir hoffen, damit einen wertvollen Beitrag zum Gemeinwohl zu leisten. Ich sehe die DAASI International als erfolgreichen Proof of Concept für ein Open-Source-Business-Modell, in dem Werte wichtiger sind als Gewinnmaximierung.

Peter Gietz, Gründer

David Hübner &
Markus Widmer

# VORWORT DER GESCHÄFTSFÜHRER

Die Wurzeln der DAASI International liegen in Dienstleistungen im Bereich Identity & Access Management für die Forschung – einem Umfeld, das von Offenheit, Innovation und Nachhaltigkeit lebt. Diese Werte haben uns von Anfang an geleitet und prägen bis heute unsere Arbeit. Im Mittelpunkt unserer Philosophie stehen Open Source, Datenschutz und offene Standards.

Im Jahr 2025 hat die DAASI International ihr 25. Jubiläum gefeiert. Sie ist in dieser Zeit stetig gewachsen und konnte dabei zunehmend auch Kunden aus öffentlicher Verwaltung und Industrie von diesen Werten überzeugen. Das zeigt uns, dass digitale Souveränität immer stärker in der Mitte der Gesellschaft ankommt, und es bestärkt uns in unserer Mission.

Wir sind überzeugt, dass nur durch transparente, offene und herstellerunabhängige Lösungen echte Kontrolle über IT-Infrastrukturen möglich ist. In einer Zeit, in der diese Kontrolle zunehmend bei einigen wenigen Großkonzernen liegt, sehen wir uns als europäisches Gegengewicht zu dieser Entwicklung. Wir möchten unseren Kunden sichere, innovative und effiziente IAM-Lösungen anbieten, welche ihre digitale Souveränität bewahren. Durch unsere jahrzehntelange Erfahrung und Expertise können wir dabei flexible und an individuelle Herausforderungen angepasste Lösungen realisieren.

IT bedeutet auch immer Fortschritt. Dieser hat sich in den letzten Jahren nochmals spürbar beschleunigt. Als forschungsnahes Unternehmen verfolgen wir diese Entwicklungen aufmerksam, um neue Standards oder technische Verbesserungen intelligent in unsere Produkte und Arbeitsabläufe zu integrieren, ohne dabei Stabilität und Kontinuität aus dem Blick zu verlieren.

Open Source lebt von Kooperation und Fairness, und wir fassen dies auch stets als soziale und gesellschaftliche Aufgabe auf. Unseren Mitarbeiter*innen möchten wir einen guten, interessanten und sicheren Arbeitsplatz bieten und durch unser Engagement in Verbänden, Forschungsnetzwerken, Open-Source-Projekten sowie durch unser großes Partnernetzwerk die Zusammenarbeit in der Community stärken.

D. Hübner Widmer

David Hübner und Markus Widmer, Geschäftsführer

# Warum OPEN SOURCE?

Open Source is happening! Auch etablierte Tech-Konzerne, die sogenannten Global Player wie Amazon und Google, unterstützen aktiv Open-Source-Projekte und setzen bei ihren Lösungen auf offene Technologien. Wir sagen Ihnen, warum:

## FREI, UNABHÄNGIG, NACHHALTIG

Proprietäre Software unterliegt stets kostenpflichtigen Lizenzen. Der Quellcode ist lediglich für den Hersteller einsehbar und darf nur durch diesen verändert werden. Die Entwicklung neuer Features richtet sich nach der allgemeinen Nachfrage am Markt; eigene Weiterentwicklungen sind nicht möglich. Bei Open-Source-Software haben Sie hingegen freien Zugang zum Quellcode und können neue Funktionalität bei Bedarf selbst oder mithilfe des IT-Dienstleisters Ihrer Wahl integrieren sowie weitere Anpassungen vornehmen. Offene Standards sorgen für mehr Kompatibilität mit anderen Systemen und der Wegfall von Lizenzgebühren entlastet obendrein Ihr Budget. Mit Open-Source-Lösungen fördern Sie Innovation, skalieren Ihre Technologien und schonen Ihre finanziellen Ressourcen. Darüber hinaus sind Sie unabhängig und geben selbst Zeitpunkt und Richtung für etwaige Modifikationen vor.

= **UNABHÄNGIGKEIT**

= **HOHE FLEXIBILITÄT UND ANPASSBARKEIT**

= **TRANSPARENZ**

= **OFFENE STANDARDS**

## AUS ÜBERZEUGUNG OPEN SOURCE

Wir stehen fest hinter der Open-Source-Idee, weil wir der Überzeugung sind, dass dieses Prinzip nicht nur die Grundlage für digitale Souveränität bildet, sondern auch für Innovation, Fortschritt und Effizienz. Open Source leistet einen wichtigen Beitrag, um die digitale Kluft sowohl zwischen verschiedenen Gesellschaftsschichten als auch zwischen den Ländern des globalen Nordens und Südens zu verringern. Die DAASI International arbeitet seit vielen Jahren eng mit Entwickler*innen moderner Open-Source-Software im IAM-Bereich zusammen, setzt sich in verschiedenen Gremien für Standardisierungen ein und entwickelt selbst ausschließlich Produkte, die einer Open-Source-Lizenz unterliegen. Zudem trägt sie aktiv dazu bei, dass Open-Source-Technologien auch in Afrika sinnvoll eingesetzt werden.

Die DAASI International legt großen Wert auf strukturiertes und flexibles Projektmanagement, das die Zusammenarbeit für alle Beteiligten angenehm und transparent gestaltet. Deshalb arbeiten die Teams nach der agilen Projektmanagementmethode Scrum. Erreichen Sie Ihr Ziel mit uns gemeinsam – Schritt für Schritt.

# Agiles **PROJEKT MANAGEMENT**

## FLEXIBEL

Wir teilen Projekte in vierwöchige Projektphasen ein, sogenannte „Sprints". Nach jedem Sprint wird die bisherige Arbeit im Team evaluiert und die nächste Projektphase geplant. Dadurch fließen stets neue Erkenntnisse in die Projektarbeit ein, die zur Optimierung des Projektverlaufs beitragen. So entsteht eine iterative Arbeitsweise, die auf Anforderungsänderungen flexibel reagieren kann.

## TRANSPARENT

Die Stakeholder erfahren stets, in welchem Stadium sich ihr Projekt befindet. Sie erhalten permanentes Feedback und können bereits früh Ergebnisse sehen und so etwaige Anpassungen vornehmen lassen.

## NACHHALTIG

Die zyklischen Sprint-Meetings gewährleisten den regelmäßigen Austausch der Teammitglieder im laufenden Projekt. Dies sorgt für klare Strukturen während des Arbeitsprozesses und stellt nicht nur die Qualität des Endergebnisses nachhaltig sicher, sondern auch die Produktivität und Zufriedenheit aller Projektpartner.

## FESTPREISPROJEKTE

Diese bieten wir an, wenn Sie mit exakten Budgetvorgaben arbeiten. Da Leistungsumfang und Leistungszeitraum im Voraus genau berechnet werden müssen, dauert die Planungsphase meist etwas länger. Zur Berechnung des Festpreises nutzen wir Ihre Lastenhefte oder Spezifikationen, wie eine Anforderungsanalyse oder ein Konzept für eine Implementierung.

## AUFWANDSPROJEKTE

Wir erstellen für Sie eine Kostenprognose. Der finale Preis ist schließlich abhängig vom tatsächlichen Arbeitsaufwand. Da die Planungsphase weniger Zeit in Anspruch nimmt, profitieren Sie von einem schnelleren Projektstart. Zudem können wir bei Projekten nach Aufwand flexibler auf Konzeptänderungen und neue Anforderungen während der Arbeitsphase reagieren.

# DAASI International ist Expertin für IDENTITY & ACCESS MANAGEMENT

Im Zuge der fortschreitenden Digitalisierung stehen Organisationen vor der Herausforderung, eine Vielzahl digitaler Identitäten effizient und sicher zu verwalten. Diese Identitäten umfassen Daten und Konten von Beschäftigten sowie von externen Nutzer*innen (wie Kunden- und Lieferorganisationen) und zunehmend auch von Diensten und Geräten (Internet of Things). Identity & Access Management (IAM) ermöglicht es, Benutzer*innen an zentraler Stelle mit allen erforderlichen Accounts und Zugriffsrechten auszustatten. Auf diese Weise werden sensible Ressourcen vor unbefugten Zugriffen geschützt, ohne dass dabei ein größerer Verwaltungsaufwand entsteht.

**Föderiertes Identity & Access Management mit Open-Source-Software ist die Kernkompetenz der DAASI International**.

## MIT IAM ZU MEHR EFFIZIENZ UND SICHERHEIT

Verfügt eine Organisation über mehrere Systeme und mehr als ein paar Dutzend Benutzer*innen, ist es sinnvoll, sich mit der systematischen Identitätsverwaltung auseinanderzusetzen. Für jedes System erhalten Benutzer*innen einen Account, der über ein Passwort und weitere Authentifizierungsfaktoren gesichert ist. Konventionelles Nutzermanagement speichert und verwaltet diese Daten meist in verschiedenen, voneinander getrennten Datenbanken. Dies führt zu unübersichtlichen Strukturen sowie zu Mehrfachadministration und kostet Nutzer*innen wie Administrator*innen unnötig viel Zeit. Zudem entsteht ein Sicherheitsrisiko, wenn Accounts, etwa von ausgeschiedenen Mitarbeiter*innen, nicht konsequent und zeitnah deaktiviert werden können.

Mit IAM werden viele Systeme von einer einzigen zentralen Benutzerdatenverwaltung gesteuert. Die Komplexität wird so deutlich reduziert und eine schnelle Bereitstellung von Accounts und Zugriffsrechten ermöglicht. Organisationen und Nutzer*innen profitieren darüber hinaus von höherer Datensicherheit und einer verbesserten User-Experience, etwa durch Single Sign-On und Self-Service.

## FÖDERATIONEN – RESSOURCEN ALLEN ZUGÄNGLICH MACHEN

Im föderierten IAM können Benutzer*innen nicht nur auf die Ressourcen ihrer eigenen Organisation zugreifen, sondern auch auf die Ressourcen anderer Organisationen innerhalb der Föderation. Dabei verwenden sie ihre bereits vorhandenen Zugangsdaten für die Authentifizierung und müssen keine zusätzlichen Accounts bei der Partnerorganisation erstellen. Solche Föderationen werden durch Verträge gebildet, die die Aktualität der Daten sowie die datenschutzkonforme Verarbeitung sicherstellen, und basieren auf einer Zertifikatsliste der beteiligten Server, die als Mitgliederverzeichnis fungiert.

## DIE TECHNOLOGIE

Identity & Access Management macht sich verschiedene Technologien zunutze, um die automatisierte Synchronisierung eines zentralen Datenstamms aus unterschiedlichen Quelldatenbanken zu ermöglichen. Dieser wird zentral in einer Datenbank oder in einem Verzeichnis gespeichert, hier „Metadirectory" genannt. Darin können nicht nur die Benutzerdaten, sondern auch die jeweiligen Zugriffsrechte direkt verwaltet, Accounts gesperrt und Passwörter neu gesetzt werden. Die aggregierten Daten werden sofort über verschiedene standardisierte oder proprietäre Protokolle in Zielsysteme übertragen. Je nach Art der Datenübertragung kommen dabei unterschiedliche Provisionierungsstrategien und Protokolle zum Einsatz:

**Just in Case** (*bevor* Nutzer*innen auf Dienste zugreifen): SPML, SCIM, regelmäßige LDAP-Abfragen, oder beliebige proprietäre Protokolle, wie die Befüllung von relationalen Datenbanken über SQL-Statements

**Just in Time** (*während* Nutzer*innen auf Dienste zugreifen): SAML, OIDC/OAuth2, oder LDAP-Abfragen nach Login

Unsere Produkte

# IDM-LÖSUNGEN

midPoint

midPoint ist die umfassende Open-Source-Software für „Identity Governance and Administration“ und wird als Standardprodukt im Identity Management eingesetzt. Als Komplettlösung verfügt midPoint über alle nötigen Tools und Konfigurationsmöglichkeiten, die für die Einführung Ihres IAM-Systems benötigt werden – und mehr. Die DAASI International ist offizieller Gold-Partner des midPoint-Entwicklers Evolveum.

**Credential Management:** Automatische Generierung von starken Passwörtern nach Vorgabe der Administrator*innen, für ein hohes Maß an Sicherheit.

**Workflow:** midPoint kann sehr einfach an existierende Prozesse des Authorisierungs-Workflows angepasst werden. Dies stellt sicher, dass der Arbeitsablauf nicht gestört wird, das System jedoch vor unberechtigten Zugriffen geschützt ist.

**Organisationsstruktur:** Ein in midPoint integriertes Strukturmodell sorgt für die einfache Anpassung der Software an die Strukturen und Hierarchien innerhalb Ihrer Organisation.

**Identity Governance:** Die Verwaltung von Identitäten ist mehr als die reine Technologie, sie umfasst auch wesentliche Geschäftsprozesse. Verwalten Sie die Rollen und Zugangsrechte Ihrer Benutzer*innen gemäß betriebsinterner Richtlinien.

**Auditing:** Für Transparenz und Nachvollziehbarkeit von Interaktionen. Alle Entscheidungen werden konstant durch einen Feedback-Mechanismus überprüft, um im Bedarfsfall die zuständigen Stellen zeitnah benachrichtigen zu können.

**Entitlement:** Bestimmen Sie die Verwaltung individueller Zugriffsrechte auf allen Ebenen (User, Rollen, Projekte, Hierarchien), um Ihre Ressourcen zu schützen.

Mit OpenLDAP gibt es eine Open-Source-Lösung für die zentrale Benutzerverwaltung. Die Software integriert den IEFT-Standard LDAPv3 und dient als Referenzsystem für andere Implementierungen. OpenLDAP ist einer der leistungsfähigsten LDAP-Server. Er kann sich selbstständig an die Leistungsfähigkeit der Hardware anpassen und verleiht so jeder IT-Infrastruktur mehr Stabilität. OpenLDAP ist ein Open-Source-Gemeinschaftsprojekt. Eine weltweite Community arbeitet stetig an dessen Optimierung, mit dem Ziel einer umfassenden Open-Source-LDAP-Suite. Die Entwicklung von OpenLDAP wird von Symas organisiert, einer US-amerikanischen Partnerfirma der DAASI International. Symas setzt dabei auf bewährte Open-Source-Software, wie OpenSSL, Cyrus SASL, Heimdal Kerberos oder Berkeley DB und bietet zudem mit der Datenbank LMDB oder dem Hashverfahren PBKDF2 zeitgemäße Technologien für bessere Performanz und höhere Sicherheit an.

eduMFA ist ein innovatives Authentifizierungssystem für Multi-Faktor-Authentifizierung, das insbesondere auf die Bedürfnisse von Hochschulen zugeschnitten wurde. Durch die Integration mehrerer Authentifizierungswege bietet eduMFA flexiblen Schutz sensibler Daten. Der von deutschen Hochschulen erstellte Fork der Open-Source-Software privacyIDEA ist modular aufgebaut und kann individuell angepasst und erweitert werden. Dank der hohen Skalierbarkeit und der Unterstützung für Mandanten- und Multi-Instanz-Umgebungen eignet sich eduMFA für Organisationen beliebiger Größe. Die Anpassung des Authentifizierungsflows ist flexibel machbar, da die Kommunikation über gängige REST-Schnittstellen erfolgt. Dies ermöglicht eine nahtlose Integration in bestehende IT-Infrastrukturen. eduMFA unterstützt außerdem eine Vielzahl von Authentifizierungstokens. Besonders hervorzuheben ist die Implementierung von Passkeys, welche eine Authentifizierung ohne Passwort oder Eingabe des Nutzernamens ermöglicht und gleichzeitig durch Verifizierung der Gegenstelle effektiven Schutz gegen Phishing bietet.

didmos ist die IAM-Suite der DAASI International. Ihre Stärke liegt in der modularen Form: Sie besteht aus sieben anpassbaren Open-Source-Modulen, die über Plugin-Schnittstellen erweiterbar sind und sich hervorragend ergänzen. Zusammen bilden sie ein leistungsstarkes, standardkonformes IAM-System. Alle Module sind unabhängig voneinander einsetzbar und können einzeln in bestehende Infrastruktur integriert werden.

## Das IAM-Framework
## DIDMOS

CORE

didmos Core ermöglicht die Verwaltung von Objekten, Benutzern und Gruppen. Das Python-basierte Modul nutzt das Django-Framework für teilweise automatisiertes Schreiben von App-Codes, was den Entwicklungsprozess vereinfacht. Core stellt SCIMv2-Endpunkte für die Verwaltung und Abfrage von Identitätsdaten sowie weitere REST-Endpunkte für mehrstufige Workflow-Implementierungen und rollenbasierte Zugriffskontrolle (RBAC). Ein Metadirectory in Form eines LDAP-Servers fungiert als hochperformantes Daten-Backend, das didmos Core zur Webservice-Schnittstelle macht, um LDAP-Daten zu schreiben, auszulesen und Business-Logiken zu implementieren.

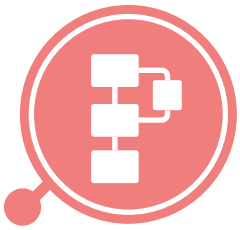
LUI

Das LDAP User Interface, kurz LUI, ist die Frontendkomponente zur Administration von Benutzer*innen und für Self-Service-Funktionalitäten, einschließlich der Selbstverwaltung eigener MFA-Tokens. Durch die Unterstützung des SCIMv2-Standards zur Verteilung von Identitäten in der Cloud kann LUI universell auch für andere IdM-Backends eingesetzt werden. LUI ist auf vielen Ebenen individualisierbar und lässt sich ganz einfach an Ihr Corporate Design anpassen.

ETL FLOW

ETL Flow (Extract, Transform, Load, Workflow) sorgt für die Extrahierung von Daten aus verschiedenen Quellen – etwa aus ERP-, SAP-, XML- oder SQL-Datenbanken – die schließlich in das zentrale Metadirectory synchronisiert werden. Entscheidende Prozesse sind dabei die Identifizierung von Identitäten anhand gewichteter Attribute (Duplikaterkennung), die Zusammenführung zu einem konsistenten Datensatz mit weiteren automatisch gebildeten Attributen, automatische Gruppenbildung und Attributerzeugung, etwa für E-Mail-Adressen.

Der didmos Provisioner ermöglicht die Übertragung von Identitätsinformationen in angeschlossene Zielsysteme in Echtzeit. Relevante Änderungen werden als JSON-Dokument in das Queueing-System RabbitMQ geschrieben und schließlich von einem dedizierten Worker in das Zielsystem eingespielt. Dabei greift der Worker auf das ICF-Konnektor-Framework zurück, wodurch verschiedene Schnittstellen, wie SOAP, REST, LDAP oder SQL bedient werden. Zur Anbindung proprietärer Systeme können auch eigene Konnektoren entwickelt werden.



PROVISIONER

Der Authenticator ist Identityprovider (IdP) und Authentifizierungskomponente und kann an individuelle Anforderungen innerhalb jeder SSO-Umgebung angepasst werden. Die Integration der Protokolle SAML und OpenID Connect ermöglicht es Benutzer*innen, sich sowohl über lokale als auch externe Accounts, z. B. via Social-Login, anzumelden. Sie können dabei auf alle Dienste innerhalb einer Föderation zugreifen, ohne mehrere Accounts anlegen und verwalten zu müssen. Für maximale Datensicherheit durch Multi-Faktor-Authentifizierung lässt sich der Authenticator mit eduMFA verbinden.

AUTHENTICATOR

Die didmos Federation Services sind das neueste Modul dieser IAM-Suite. Ein Toolkit, das insbesondere die Herausforderungen in föderierten IAM-Umgebungen adressiert, wie die Integration zahlreicher Identity-Provider oder die Bewältigung von Authentifizierungsfragen im Non-Web-Bereich. Das erste Tool, FedSSH, sichert SSH-Zugriffe auf Server über den Login an föderierten IdPs ab. Komplexe IT-Landschaften wie Forschungsinfrastrukturen können hiervon in puncto Sicherheit, Benutzerfreundlichkeit und Administrationsaufwand besonders profitieren.

FEDERATION SERVICES

Der Pwd Synchroniser synchronisiert Passwortänderungen eventbasiert an einem Active Directory Domain Controller in andere Verzeichnisse, wie OpenLDAP. Die einfache Installation als Windows-Dienst, die verschlüsselte Zwischenspeicherung auf dem Domain-Controller sowie die Protokollierung der Synchronisierungsvorgänge machen den Pwd Synchroniser zu einem effektiven Modul zur Integration von Active Directory.

PWD SYNCHRONISER

Unsere Produkte

# SSO-Technologien

## Shibboleth

Shibboleth stellt föderierte Authentifizierung und Autorisierung für Webanwendungen bereit und kommt insbesondere in Verbünden von Hochschulen, Behörden und großen Organisationen zum Einsatz. Die Lösung basiert primär auf dem SAML-Standard und ist als Open-Source-Projekt breit etabliert. Die Weiterentwicklung wird durch das Shibboleth Consortium koordiniert, in dem auch DAASI International Mitglied ist.

Shibboleth ermöglicht Single Sign-on (SSO), sodass Nutzende nach einmaliger Anmeldung auf mehrere angebundene Dienste zugreifen können – auch organisationsübergreifend innerhalb von Föderationen. Dabei werden, gemäß dem Prinzip der Datensparsamkeit, nur die jeweils erforderlichen Attribute an Dienste übertragen.

Shibboleth umfasst zwei zentrale Komponenten:

1. Der Shibboleth Identity Provider (IdP) ermöglicht einen zentralen Login, über den sowo gene Dienste als auch Anwendungen inner einer Föderation angebunden werden kör

2. Der Shibboleth Service Provider (SP) scl Webanwendungen, indem er die Verarbei des komplexen SAML-Protokolls überni sodass diese nicht selbst implementiert we muss.

Auf Wunsch erweitert DAASI International Standardfunktionen von Shibboleth, beispiel se durch Plugins für Multi-Faktor-Authentifizie (etwa mit eduMFA) oder zur Integration mode Protokolle wie OpenID Connect.

## KEYCLOAK

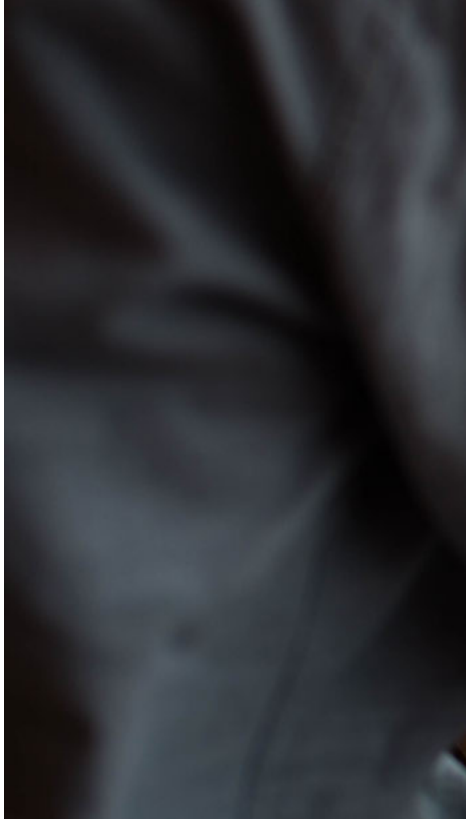
Keycloak ist ein leistungsfähiger Open-Source-Identity-Provider, der als zentrale Authentifizierungsplattform dient und Single Sign-on über alle angebundenen Applikationen ermöglicht. Gleichzeitig vereinfacht er die Verwaltung von Benutzerkonten sowie die Umsetzung von Self-Service-Funktionen für Registrierung und Passwortmanagement. Die Rechtevergabe erfolgt über Role-Based Access Control (RBAC), wodurch sich auch komplexe Berechtigungsstrukturen effizient abbilden lassen. Als Community-Version von Red Hat SSO basiert Keycloak auf etablierten Standards wie OpenID Connect (OIDC), OAuth 2.0 und SAML und lässt sich dadurch flexibel in bestehende Systemlandschaften integrieren. Individuelle Anforderungen können bei Bedarf durch Erweiterungen (Plugins) umgesetzt werden.

Keycloak profitiert von einer sehr aktiven Community, die das Produkt kontinuierlich weiterentwickelt und an neue Bedarfe anpasst.

## SATOSA

Das Authentifizierungstool Satosa ähnelt Shibboleth auf den ersten Blick sehr. Tatsächlich ist Satosa aber ein Proxy, der zwischen einen Dienst und einen Identity Provider (IdP) geschaltet wird. Dieser Proxy besteht aus zwei Komponenten, die jeweils mit dem Dienst oder dem IdP sowie untereinander kommunizieren. Satosa ermöglicht es, die Kommunikation zwischen Dienst und IdP transparent weiterzuleiten oder zu modifizieren. Dabei können Attribute geändert oder von zusätzlichen Datenbanken abgefragt werden. Es ist sogar möglich, das Authentifizierungsprotokoll zu wechseln, wodurch die Kommunikation in einigen Fällen erst ermöglicht wird.

Satosa unterstützt Single Sign-On über die Protokolle OpenID Connect und SAML hinweg, ohne dass Benutzer*innen dies bemerken.



## Expertise im Bereich IAM

# UNSERE LEISTUNGEN

Als Full-Service-Provider begleitet Sie die DAASI International von der ersten Überlegung an, über Konzeption, Entwicklung, Migration und Schulung, bis hin zum Support in den Produktivbetrieb. Wir sind für Sie da – in jeder Phase Ihres IAM-Projekts.

### CONSULTING

Die DAASI International steht Ihnen bei Ihrem Vorhaben beratend zur Seite. Wir evaluieren den Ist-Zustand Ihrer IT-Infrastruktur, erstellen Bedarfsanalysen sowie Grob- und Feinkonzepte, führen Machbarkeitsstudien durch und beantworten Ihre Fragen zu IT-Sicherheit und Projektmanagement.

### INTEGRATION

Jede Neueinführung von IT-Systemen birgt Herausforderungen. Die DAASI International geht diese gemeinsam mit Ihnen an. Wir integrieren neue Anwendungen in unterschiedlichste IT-Systeme, strukturieren diese bei Bedarf neu und passen sie an Ihre Prozesse wieder optimal an. Wir bauen Föderationen auf oder integrieren Fremd-Systeme in bereits bestehende Föderationen.

### SOFTWAREENTWICKLUNG

Die gewählte Standardlösung passt nicht zu Ihrer IT-Landschaft oder kann Ihre Anforderungen nicht umfassend erfüllen? DAASI International entwickelt kundenspezifische Plugins, Overlays und Konnektoren für bestehende Produkte, erstellt Lastenhefte und evaluiert Softwarebibliotheken. Lassen Sie die Software von uns nach Ihren Wünschen anpassen. Gerne entwickeln wir auch individuelle Lösungen für Sie.

## SCHULUNGEN

Als Botschafterin für IAM mit Open-Source-Technologie gibt die DAASI International ihr Wissen auch gerne weiter. Unsere IAM-Expert*innen schulen Ihr Personal zu verschiedenen Themen, wie LDAP, SAML, OIDC und OAuth2 sowie zu unseren Open-Source-Lösungen. Für eine zielgerichtete Wissensvermittlung passen wir das Präsentationsmaterial individuell an und stellen Schulungsunterlagen zur Verfügung.

## SUPPORT

Nach der Einführung eines neuen Systems kommen gerade in der Anfangsphase viele Fragen auf und für den reibungslosen Betrieb ist eine regelmäßige professionelle Wartung unerlässlich. Deshalb ist die DAASI International auch nach Projektabschluss weiterhin für Sie da. Wir bieten Ihnen zuverlässigen Support für Ihre maßgeschneiderten Lösungen sowie für alle unsere Standardprodukte. Gerne beantworten wir Ihre Fragen über unseren Helpdesk. Im Rahmen unserer Managed Services erhalten Sie auf Wunsch ein umfassendes Betriebspaket, inklusive Hosting, Backup und Monitoring, für Ihren Produktivdienst als Software as a Service.

Unsere Kunden

# ERFOLGSGESCHICHTEN

## DAS PROJEKT

Gewünscht wurde die Bereitstellung einer IDaaS-Plattform für kommerzielle Partner der ESA in den ESA-Mitgliedsstaaten, um ihnen so Zugriff auf Anwendungen und Erdbeobachtungsdaten der Agency zu gewähren.

## DIE SPEZIFIKATIONEN

Die Nutzer*innen sollten über ein Gluu-basiertes System eine zentrale ESA-Identität erhalten. Die Plattform musste Kontoverwaltung und SSO ermöglichen und dafür Standards wie SAML, OpenID Connect und OAuth unterstützen sowie hochverfügbar sein.

## HERAUSFORDERUNGEN

Die Geschäftskontinuität zu gewährleisten, erforderte eine hochverfügbare Plattform. Arbeitsabläufe mussten automatisiert, die Kontenübertragung verlustfrei sichergestellt werden.

## UNSER BEITRAG

Gemeinsam mit Projektpartner Deimos entwickelte die DAASI International eine hochverfügbare Plattform mit einem Message-Queue-System zur sicheren Datenübertragung. Arbeitsabläufe zwischen den Anwednungen didmos, Jira und Gluu wurden automatisiert, die Sicherheit durch die zentralisierte Benutzerverwaltung erheblich verbessert. Im Anschluss an das Projekt betrieben DAASI International und Deimos die Plattform für mehrere Jahre weiter und unterstützten die Integration neuer Dienste.

## DAS PROJEKT

Das Identity-Management-System der Nikolauspflege war in die Jahre gekommen. Die Stiftung entschied deshalb, ihr System durch eine moderne Standardlösung zu ersetzen.

## DIE SPEZIFIKATIONEN

Verantwortlichkeiten mussten sinnvoll aufgeteilt werden. Die Gewährleistung von Sicherheit, Datenschutz und die Einhaltung der BSI-Richtlinien erforderten ein 4-Augen-Prinzip. Zudem sollte die Administration entlastet, Prozesse beschleunigt und die Nutzererfahrung durch eine barrierefreie Oberfläche verbessert werden.

## HERAUSFORDERUNGEN

Es galt, die langjährige Individualprogrammierung ohne detaillierte Dokumentation durch eine Standardsoftware abzulösen und inkonsistente Personaldatensätze aufzuarbeiten.

Nikolauspflege

## UNSER BEITRAG

Um den Spezifikationen nachzukommen, wurden Verwaltungsrechte auf verschiedenen Ebenen sowie Key-User-Rollen implementiert. Mithilfe eines Workflows für Berechtigungsanträge wurde das 4-Augen-Prinzip etabliert. Barrierefreiheit unterstützt midPoint standardmäßig. Vereinzelte Übersetzungslücken wurden durch spezielle Erweiterungen ergänzt. Mit der Zusammenführung der verschiedenen Datenbestände in ein IdM-System wurde die Verwaltung domänenübergreifender Berechtigungen automatisiert und so stark vereinfacht.

## DAS PROJEKT

Beauftragt wurde der Aufbau einer Webportal-Lösung zur Registrierung und Verwaltung von Kundenbenutzer*innen, sodass sich diese für ausgesuchte Anwendungen zentral registrieren und ihre Daten selbst verwalten können.

## DIE SPEZIFIKATIONEN

Die Konzeption des Portals sah eine On-Premises-Lösung vor, die DSGVO-konform sein und typische Self-Service-Funktionalitäten wie Accountregistrierung, Passwortänderung und die Möglichkeit der Beantragung weiterer Dienste mitbringen sollte. Zudem wurde die Interaktion zwischen dem Portal und dem bereits vorhandenen LDAP-Server gewünscht, welcher die Daten zur Autorisierung externer Benutzer*innen bereitstellt.

## HERAUSFORDERUNGEN

Das System sollte so gestaltet sein, dass Administrator*innen unbegrenzt weitere Anwendungen integrieren können, ohne zukünftig externe Dienstleister für Konfigurationsarbeiten zu benötigen.

**Staatsbibliothek zu Berlin**
Preußischer Kulturbesitz

## UNSER BEITRAG

Die DAASI International baute dieses Portal auf Basis von LUI, einem kundenspezifisch anpassbaren Modul des IAM-Frameworks didmos, neu auf. Es besteht aus zwei Komponenten: einem Self-Service- und einem Administrationsportal für die Verwaltung externer Benutzer*innen. didmos LUI fungiert hierbei als Schnittstelle zwischen den Webanwendungen und dem OpenLDAP-Server.

Unsere Kunden

# WEITERE REFERENZEN

CIANDO Mediengruppe Stein

KIT Karlsruhe Institute of Technology

FRANKFURT UNIVERSITY OF APPLIED SCIENCES

COMMERZ BIBLIOTHEK seit 1735

UNIVERSITÄT ERFURT

LEUPHANA UNIVERSITÄT LÜNEBURG

Technische Universität Braunschweig

MAX-PLANCK-INSTITUT FÜR BIOPHYSIK

STATISTIK AUSTRIA Die Informationsmanager

OSB Open Source Business ALLIANCE

GÉANT

Universität Konstanz

Kunsthochschule Bayern

Cornelsen

GWDG Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

# INFRASTRUKTUR
## im Bereich der Digital Humanities

Die DAASI International hat es sich zur Aufgabe gemacht, Geisteswissenschaftler*innen bei der Vernetzung und der Verwendung moderner digitaler Methoden zum Erkenntnisgewinn – Digital Humanities – umfassend zu unterstützen und die Entwicklung von entsprechenden Tools zu fördern. Hierzu entwickelt und implementiert sie innovative Authentifizierungs- und Autorisierungsinfrastrukturen (AAIs) sowie Datenbanken und Visualisierungstools und konzipiert nachhaltige Betriebsmodelle.

## DARIAH-DE

DARIAH-DE ist der deutschsprachige Teilbereich des europäischen Infrastruktur-Projekts „Digital Research Infrastructure for the Arts and Humanities" (DARIAH). Ziel dieses Projekts ist es unter anderem, eine Infrastruktur für virtuelle Forschungsumgebungen für Geisteswissenschaftler*innen bereitzustellen, um neue digitale Forschungsmethoden zu entwickeln. DARIAH-DE unterstützt diesen Aufbau durch Beratung, die Verknüpfung von bisher getrennten Aktivitäten und über generische Dienste der technischen Infrastruktur. Digitale Ressourcen, Anwendungen und Erkenntnisse werden unabhängig der Disziplin gemeinsam genutzt und miteinander verknüpft. Neben Aufbau und Betrieb der AAI, der Integration neuer Technologien und der Entwicklung nachhaltiger Betriebskonzepten hat die DAASI International auch bei Konzeption und Aufbau der DARIAH-Storage-Infrastruktur mitgewirkt.

## TextGrid

TextGrid ist eine virtuelle Forschungsumgebung für alle textbasiert arbeitenden Disziplinen der Geisteswissenschaften. Sie dient als Werkzeug für wissenschaftliche Editionsarbeit, bietet Module für die methodische, kollaborative Textdatenverarbeitung an und verfügt über standardisierte Schnittstellen zu Publikationssoftware, Forschungsdaten und -tools. Hinter TextGrid steht die Vision eines digitalen Ökosystems für die geisteswissenschaftliche Forschung, in dem ein freier Austausch sowie eine spezifische Anpassung einzelner Komponenten je nach den Bedürfnissen der Fach-Community möglich sind. Die DAASI International war am Aufbau des Nutzermanagements sowie der Rechte- und Lizenzverwaltung von TextGrid beteiligt. Auch die Entwicklung der Workflow-Oberfläche und des Datenrepositoriums inklusive AAI haben wir mitwirkend begleitet. Inzwischen ist TextGrid Teil des Angebots von DARIAH-DE.

## NFDI4Culture

NFDI4Culture ist eines der geisteswissenschaftlichen Konsortien innerhalb der Nationalen Forschungsdateninfrastruktur (NFDI) und adressiert Forschungsdaten aus den Bereichen Kunst, Musik, Architektur, Theater, Film und Medien. Ziel des Projekts ist es, verteilte Datenbestände systematisch zu erschließen, nachhaltig zu sichern und für die wissenschaftliche Nutzung zugänglich zu machen. Dazu werden Standards, Werkzeuge und Dienste für das Forschungsdatenmanagement entwickelt und bereitgestellt. Die DAASI International unterstützt das Projekt beim Aufbau einer föderierten Authentifizierungs- und Autorisierungsinfrastruktur (AAI) unter Einbeziehung von Lizenzmanagement sowie bei der Integration und Anbindung bestehender Lösungen.

# USER-ZENTRIERTE IDENTITÄT

## in Forschung und Lehre

Zunehmend zeichnet sich der Trend ab, Identität nicht mehr primär organisationsbezogen zu denken, sondern vom Individuum und dessen informationeller Selbstbestimmung auszugehen. Im Bereich Forschung und Lehre etabliert sich daher europaweit das Konzept einer lebenslangen Identität, unabhängig von der jeweiligen Heimateinrichtung. DAASI International engagiert sich in diesem Kontext in zwei Projekten:

## eduID

Im Zentrum moderner digitaler Forschungsinfrastrukturen steht die Frage, wie digitale Identitäten über Institutionsgrenzen hinweg verlässlich und langfristig nutzbar bleiben. Die eduID gibt darauf eine überzeugende Antwort: Sie etabliert eine dauerhafte, persönliche digitale Identität, die unabhängig von einzelnen Einrichtungen besteht und den Zugang zu wissenschaftlichen Diensten über verschiedene Stationen hinweg ermöglicht. Gerade in einem Umfeld, das von internationaler Mobilität und häufigen institutionellen Wechseln geprägt ist, schafft sie Kontinuität und vereinfacht den Umgang mit digitalen Ressourcen erheblich. Dabei ist die eduID kein einheitliches Produkt, sondern ein Konzept, das in vielen Ländern unter dem Namen „eduID" umgesetzt wurde – jeweils auf Basis unterschiedlicher technischer Lösungen. Ein Beispiel ist die deutsche Implementierung durch den DFN, die zeigt, wie sich solche Identitätsmodelle in bestehende nationale Infrastrukturen integrieren lassen. Gemeinsam ist diesen Ansätzen ein klarer Leitgedanke: Nutzer*innen verwalten ihre Identität selbstbestimmt und behalten die Hoheit über ihre Daten. So entsteht ein vertrauenswürdiges, föderiertes Ökosystem, das Offenheit und Sicherheit miteinander verbindet.

DAASI International hat die Software für die DFN-eduID auf Grundlage von didmos entwickelt und zur Verfügung gestellt. Das System wird kontinuierlich weiterentwickelt, um alle Anforderungen der nutzenden Einrichtungen zu erfüllen.

## BonafID

Wie das Konzept eduID auch außerhalb Europas angewendet werden kann, zeigt BonafID. Die Plattform wird in afrikanischen Forschungs- und Bildungsnetzwerken eingesetzt und übersetzt die Idee der eduID in eine konkrete, skalierbare Infrastruktur. Als cloudbasierter Dienst ermöglicht sie zum einen den Hochschulen des Landes, ihre Identitäten in einem Multimandantensystem selbst zu verwalten, und zum anderen den jeweiligen Nutzer*innen Zugriff auf im Rahmen der weltweiten Inter-Föderation eduGAIN zur Verfügung gestellte Dienste. Im Mittelpunkt steht auch hier der Mensch: BonafID setzt auf eine konsequent nutzerorientierte Gestaltung, die es Anwender*innen erlaubt, ihre Zugehörigkeiten selbst zu verwalten und ihre digitale Identität aktiv zu steuern. Gleichzeitig profitieren Organisationen von einer flexiblen „Identity as a Service"-Lösung, die den Zugang zu digitalen Angeboten vereinfacht und absichert.

Gemeinsam mit dem nigerianischen Unternehmen Datasphir hat DAASI International diese Plattform auf Grundlage von didmos entwickelt. Über die technische Umsetzung hinaus steht dabei der Aufbau nachhaltiger Strukturen im Vordergrund: Durch Wissenstransfer und enge Zusammenarbeit mit Partnern wie WACREN und GÉANT entstehen Kompetenzen vor Ort, die den Betrieb und die Weiterentwicklung solcher Infrastrukturen langfristig sichern.

# Wir engagieren uns in der **FORSCHUNG**

Die DAASI International ist 2000 aus Forschungsprojekten zu X.500 und LDAP hervorgegangen, die vom Bundesministerium für Bildung und Forschung gefördert wurden. Diese Wurzeln prägen das Unternehmen bis heute. So ist die Forschungsbeteiligung ein zentraler Bestandteil der Unternehmensidentität.

Auch als etabliertes Unternehmen beteiligt sich DAASI International kontinuierlich an innovativen Projekten. Wirtschaftlich steht dabei nicht der unmittelbare Ertrag im Vordergrund. Entscheidend sind die frühzeitige Auseinandersetzung mit neuen Technologien sowie der enge Austausch mit führenden Expert*innen. Das daraus entstehende Wissen, die gesammelten Erfahrungen und die gewachsenen Netzwerke stärken die Kompetenz des Unternehmens nachhaltig.

## PROJEKTE UND INTERNATIONALE ZUSAMMENARBEIT

Die langjährige Erfahrung fließt in die Mitwirkung an zahlreichen nationalen und internationalen Initiativen ein. Dazu zählen Projekte der D-Grid-Initiative ebenso wie das Engagement in den Bereichen Digital Humanities und Forschungsinfrastrukturen. Besonders hervorzuheben sind die vom Bundesministerium für Bildung und Forschung geförderten Projekte TextGrid und DARIAH, in denen international kompatible Authentication and Authorisation Infrastructures (AAI) für geisteswissenschaftliche Forschungsumgebungen aufgebaut wurden.

Ein Meilenstein war die Beteiligung am EU-Projekt Authentication and Authorisation for Research Collaboration (AARC). In diesem Kontext wurden grundlegende Konzepte und Blaupausen für moderne AAIs entwickelt, die heute von vielen Forschungsinfrastrukturen genutzt werden. Mit AARC TREE wurden diese Ansätze weitergeführt, aktualisiert und in die Praxis überführt, mit dem Ziel, föderierte Authentifizierungs- und Autorisierungslösungen für Forschungsinfrastrukturen effizient und interoperabel zu etablieren.

## ENGAGEMENT IN DER NFDI

Im Projekt IAM4NFDI bringt DAASI International ihre AAI-Expertise in die Nationale Forschungsdateninfrastruktur (NFDI) ein. Im Mittelpunkt dieses etablierten NFDI-Basisdienstes stehen die Anbindung der verschiedenen Fachkonsortien, um deren Nutzer*innen einen föderierten Zugang zur Verfügung zu stellen, zu eigenen sowie zu Konsortium-übergreifenden Ressourcen.

Eine weitere von DAASI International unterstützte NFDI-Aktivität ist der Aufbau eines neuen Basisdienstes zu Accounting. Dabei werden Nutzungs- und Zugriffsdaten erfasst und ausgewertet, um Transparenz zu schaffen, Ressourcen gerecht zu verteilen, Prozesse nachvollziehbar zu machen und die Steuerung der föderierten Infrastruktur insgesamt zu verbessern.

## AUSTAUSCH, INNOVATION UND NACHWUCHSFÖRDERUNG

Die DAASI International beteiligt sich aktiv am internationalen Fachdiskurs und ist Mitorganisatorin der jährlich stattfindenden TIIME Unconference. Dort diskutieren IAM-Expert*innen aus der ganzen Welt aktuelle Entwicklungen, neue Technologien und zukünftige Herausforderungen der Identitäts- und Zugriffsverwaltung. Der Austausch liefert wichtige Impulse für die Weiterentwicklung zukunftsträchtiger IAM-Lösungen.

Schließlich betreibt die DAASI International eigene Grundlagenforschung im Bereich Authentication and Authorisation Infrastructures und arbeitet eng mit Universitäten und Hochschulen zusammen. Die Betreuung von Abschlussarbeiten verbindet Forschung und Praxis und trägt dazu bei, qualifizierte Nachwuchskräfte frühzeitig zu gewinnen.

DAASI International

Europaplatz 3 | 72072 Tübingen
07071 407109-0
business@daasi.de
www.daasi.de

10/2026