

DEUTSCH

CONNECTING IDEAS THROUGH OPEN SOURCE



FEDERATED IDENTITY MANAGEMENT.
DIGITAL HUMANITIES.
OPEN SOURCE.



Diese Broschüre

INHALT

ÜBER DAASI INTERNATIONAL

VORWORT DES GRÜNDERS	3
MEILENSTEINE	4
WARUM OPEN SOURCE?	6
PROJEKTMANAGEMENT	7

IDENTITY & ACCESS MANAGEMENT

EXPERTIN FÜR IAM	8
UNSERE IAM-LÖSUNGEN	10
DIDMOS	12
SSO-TECHNOLOGIEN	14
UNSERE IAM-LEISTUNGEN	16
ERFOLGSGESCHICHTEN	18

DIGITAL HUMANITIES

ÜBER DIGITAL HUMANITIES	22
UNSERE DH-TOOLS	23
UNSERE DH-LEISTUNGEN	24
UNSERE DH-PROJEKTE	25

FORSCHUNG

FOSCHUNGSBETEILIGUNG	27
----------------------	----

Peter Gietz VORWORT DES GRÜNDERS



Die DAASI International steht für Professionalität, Nachhaltigkeit, soziales Miteinander, Engagement und Fairness. Diese Werte sind tief in unserer Unternehmensphilosophie verankert und Grund dafür, warum wir zu den führenden Open-Source-Anbietern in den Bereichen Identity & Access Management (IAM) und Digital Humanities (DH) 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, interessante und abwechslungsreiche Arbeitsplätze mit innovativen Technologien für ein engagiertes Team zu schaffen. Mit der Übernahme vieler unterschiedlicher Projekte ist die DAASI International in den darauffolgenden Jahren nicht nur an Mitarbeiter*innen, sondern auch an Kenntnissen und Fähigkeiten gewachsen.

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 ermöglichen neue Arbeitsweisen. Da IAM-Technologien und -Methoden ebenfalls in virtuellen Forschungsumgebungen benötigt werden, bringen wir unser Fachwissen auch in den Digital Humanities ein und verbinden so unsere beiden Geschäftsfelder miteinander.

Durch unsere jahrelange Erfahrung, die Unterstützung und Förderung von Open Source und offenen Standards sowie durch unser Engagement in der Forschung zeichnen wir uns aus und möchten damit einen wertvollen Beitrag zum Gemeinwohl leisten.

Peter Gietz, Gründer & CEO

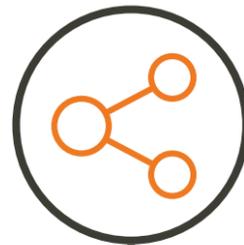
In diesem Projekt aller 9 Universitäten Baden-Württembergs war die DAASI International als externe Dienstleisterin maßgeblich beteiligt am Aufbau einer landesweiten Public-Key-Infrastructure (PKI) auf Basis von indizierten Verzeichnisdiensten mit standardisierten LDAP-Zugriffsmechanismen. Mitarbeiter*innen der DAASI International schrieben einen IETF-Internetdraft über ein LDAPv3-Schema zur Speicherung von X.509-Zertifikaten.

PKI BADEN-WÜRTTEMBERG



In Zusammenarbeit mit 17 niedersächsischen Hochschulen wurde durch DAASI International eine landesweite Lernkooperation für Studierende in Niedersachsen konzipiert und umgesetzt, die sog. Niedersachsen Authentication and Authorisation Infrastructure (Nds AAI). Die Studierenden konnten anschließend mit StudIP auf alle Ressourcen teilnehmender Hochschulen zugreifen, ohne zusätzliche Konten einrichten zu müssen.

LANDESWEITE FÖDERATION (NIEDERSACHSEN-AAI)



Die DAASI International entwickelte für verschiedene Kunden IdM-Module auf Grundlage eines OpenLDAP-basierten Metadirectory. Insbesondere bei den Arbeiten an ALOIS in Zusammenarbeit mit der Uni Augsburg, am IdM-System der UdK Berlin sowie dem System des Behördendienstleisters VRSG wurden innovative Konzepte implementiert. Diese bildeten im Nachgang die Grundlage für didmos, die IAM-Lösung der DAASI International.

GRUNDSTEINLEGUNG FÜR DIDMOS



Auf den Beitritt in das Shibboleth Consortium 2016 folgten weitere Kooperationen mit Open-Source-Entwicklern. Enge Partnerschaften wurden geschlossen mit den US-amerikanischen Unternehmen Symas, Hauptentwickler von OpenLDAP, und Gluu, Entwickler von Gluu Server. Seit 2018 beteiligt sich die DAASI International am irischen Unternehmen Crust Ltd, Hersteller der innovativen CRM- und Messaging-Plattform Crust. Die Kooperation mit midPoint-Entwickler Evolveum gipfelte 2019 in der Ernennung von DAASI International zum ersten deutschen Goldpartner.

AUSBAU PARTNERNETZWERK



2000

2002

2006

2007

2010

2014

2016

2017

2019



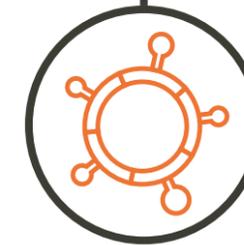
GRÜNDUNG



FORSCHUNGS-
INFRASTRUKTUREN



DARIAH-DE & AARC



DIDMOS



DIDMOS2

Der Wunsch, begonnene Forschungsarbeiten fortzuführen, führte zur Gründung der DAASI International GmbH. Sie ist ein Spin-Off des Rechenzentrums der Universität Tübingen, eine Nachfolgeorganisation von BMBF-geförderten DFN-Forschungsprojekten, die sich intensiv mit X.500 und LDAP beschäftigten – damals Forschungsgegenstand, heute in jeder größeren Organisation zu finden.

Die DAASI International war an verschiedenen Projekten wie IVOM und GAP-SLC zum Aufbau einer nachhaltigen Grid-Infrastruktur für Forschung und Entwicklung in Deutschland beteiligt. Darin wurden neue Technologien entwickelt und PKI-basierte Forschungsinfrastrukturen mit SAML-basierten Infrastrukturen interoperabel aufgebaut. In TextGrid I hat DAASI International eine AAI für das geisteswissenschaftliche D-Grid-Projekt erstellt und war an Standardisierungsinitiativen im Global Grid Forum beteiligt und damit an der Vorform von Cloud Computing.

Aufbauend auf den Ergebnissen der Projekte TextGrid II und III war die DAASI International bei DARIAH (Digital Research Infrastructure for the Arts and Humanities) am Aufbau der Infrastruktur, der Integration neuer Technologien und der Entwicklung einer nachhaltigen Betriebseinheit maßgeblich beteiligt. An Konzeption und Aufbau der DARIAH-Storage-Infrastruktur haben wir ebenfalls mitgearbeitet. Im EU-Projekt AARC hat die DAASI International DARIAH vertreten und die innovativen AAI-Konzepte entscheidend mitgestaltet.

Die DAASI International launchte mit didmos ihre eigene Open-Source-Lösung für Identity & Access Management. didmos ist ein modulares IAM-Framework, bestehend aus fünf einzeln oder kombiniert einsetzbaren Komponenten. Durch hohe Standardkonformität und die starke Ausrichtung auf Erweiterbarkeit besitzt didmos die idealen Voraussetzungen dafür, in bestehenden IT-Landschaften integriert zu werden.

In verschiedenen Projekten wurden erste Module der neusten Version von didmos eingesetzt. Während didmos1 von XML und SOAP geprägt war, handelt es sich bei didmos2 um eine Neuentwicklung auf Basis von JSON und REST. Mit dem didmos Authenticator kam ein sechstes Modul hinzu, ein auf Satosa aufbauender Proxy, der Single-Sign-on über die beiden Protokolle OpenID Connect und SAML sowie Social Login ermöglicht.

Warum OPEN SOURCE?

Open Source is Happening! Etablierte Global Player wie Amazon, Google und Twitter unterstützen aktiv Open-Source-Projekte und setzen bei ihren Lösungen längst auf Open-Source-Technologien. Wir sagen Ihnen warum.

FREI, UNABHÄNGIG, NACHHALTIG

Proprietäre Software unterliegt stets kostenpflichtigen Lizenzen. Der Source-Code ist lediglich für den Hersteller einsehbar und darf auch nur durch diesen verändert werden. Die Entwicklung neuer Features richtet sich nach der allgemeinen Nachfrage am Markt und eigene Weiterentwicklungen sind nicht möglich. Bei Open-Source-Software haben Sie 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 schont darüber hinaus Ihr Budget. Dynamisches Cloud-Computing etwa ist überhaupt nur über lizenzkostenfreie Betriebssysteme möglich. Mit Open-Source-Lösungen sind Sie unabhängig und geben selbst die Richtung vor.

AUS ÜBERZEUGUNG OPEN SOURCE

Wir stehen fest hinter der Open-Source-Idee, weil wir der Überzeugung sind, dass offene Standards die Grundlage für Innovation, Fortschritt und Effizienz bilden. Die DAASI International arbeitet daher seit vielen Jahren eng mit Entwicklern moderner Open-Source-Software im IAM-Bereich zusammen, setzt sich in verschiedenen Gremien für Standardisierungen ein und entwickelt selbst ausschließlich Produkte, die Open-Source-Lizenzen unterliegen.

Wir helfen Organisationen, ihre IT mit fortschrittlicher Technologie auf Open-Source-Grundlage effizienter und sicherer zu machen. Wir sorgen für eine verlässliche Infrastruktur, schaffen durch einfache Bedienbarkeit eine großartige User Experience – trotz zunehmender Komplexität, und ermöglichen so neue Arbeitsweisen.

+ UNABHÄNGIGKEIT

+ HOHE FLEXIBILITÄT
UND ANPASSBARKEIT

+ TRANSPARENZ

+ OFFENE STANDARDS

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

Agiles PROJEKT MANAGEMENT

FLEXIBEL

Wir teilen Projekte in zweiwöchige 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.

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 Ihnen wir an, wenn Sie mit exakten Budgetvorgaben arbeiten. Da Leistungsumfang und -zeitraum 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 für ein Konzept 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**



Organisationen stehen im Zuge zunehmender Digitalisierung vor der Herausforderung, viele digitale Identitäten effizient und sicher verwalten zu müssen. Identitäten können Daten und Accounts von Mitarbeiter*innen, Kund*innen und Lieferant*innen sein, kommen zunehmend aber auch in Form von Diensten und Dingen (Internet of Things) vor. Identity und Access Management, kurz IAM, ermöglicht es, Benutzer*innen an zentraler Stelle mit allen nötigen Accounts und Zugangsrechten auszustatten. Sensible Ressourcen sind so vor unbefugten Zugriffen geschützt – ganz ohne unübersichtlichen Verwaltungsaufwand.

Identity & Access Management sowie föderiertes IAM mit Open-Source-Software sind die Kernkompetenzen 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 bereits sinnvoll, sich mit der systematischen Identitätenverwaltung auseinanderzusetzen. Für jedes System erhalten Benutzer*innen einen Account und entsprechend viele Passwörter. Konventionelles Nutzermanagement speichert und verwaltet diese Daten meist in verschiedenen, voneinander getrennten Datenbanken. Dies führt zu unübersichtlichen Strukturen sowie zu Mehrfachadministration und kostet sowohl Nutzer*innen als auch Administrator*innen unnötig viel Zeit. Zudem entsteht ein Sicherheitsrisiko, wenn Accounts, z. B. 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 zeitnahe 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

Bei föderiertem IAM können Benutzer*innen nicht nur auf die Ressourcen ihrer eigenen Organisation, sondern auch auf die Ressourcen anderer Organisationen innerhalb der Föderation zugreifen. Für die Authentifizierung verwenden sie dabei ihre bereits vorhandenen Zugangsdaten und müssen bei der Partnerorganisation keine weiteren Accounts erstellen. Solche Föderationen werden über Verträge, die Aktualität und datenschutzkonforme Verarbeitung der Daten zusichern, sowie über ein Mitgliedsverzeichnis der beteiligten Server gebildet.

DIE TECHNOLOGIE

Identity & Access Management macht sich verschiedene Technologien zunutze, um die automatisierte Synchronisierung eines zentralen Datenstamms aus unterschiedlichen Quelldatenbanken (z. B. HR-System) zu ermöglichen. Dieser wird zentral in einer Datenbank oder einem Verzeichnis gespeichert – hier „Metadirectory“ genannt. Darin können nicht nur die Benutzerdaten selbst, sondern beispielsweise auch die jeweiligen Zugriffsrechte direkt verwaltet, Accounts gesperrt und Passwörter neu gesetzt werden. Solche aggregierten Daten werden instantan über verschiedene standardisierte oder proprietäre Protokolle in Zielsysteme provisioniert, wobei je nach Provisionierungsart unterschiedliche Protokolle zum Einsatz kommen:

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

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

Die DAASI International setzt beim Aufbau performanter IAM-Systeme, wo immer möglich, auf Open-Source-Software wie OpenLDAP, midPoint, Shibboleth, GLUU, oder das eigene IAM-Framework didmos.

Unsere Produkte

IAM-LÖSUNGEN



midPoint ist die umfassende Open-Source-Software für „Identity Governance and Administration“ und wird als Standardprodukt im Bereich Identity & Access Management eingesetzt. Als Komplettlösung und moderne Alternative zu Oracle Waveset 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 für den deutschsprachigen Raum.

Credential Management: Automatische Generierung von starken Passwörtern nach Vorgabe der Administratoren, um ein hohes Maß an Sicherheit zu gewährleisten.

Workflow: midPoint kann sehr einfach an bereits existierende Prozesse des Authentifizierungs-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 Hierarchien und Strukturen innerhalb Ihrer Organisation.

Identity Governance: Die Verwaltung von Identitäten ist nicht nur Technologie. Es geht dabei auch um Geschäftsprozesse. Verwalten Sie die Rollen und Zugangsrechte aller Benutzer*innen gemäß betriebsinterner Richtlinien und sorgen Sie so für ein hohes Maß an Sicherheit.

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

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



Gluu Server ist eine flexible Access-Management-Software, die es Ihnen ermöglicht, den Zugriff auf Ihre Ressourcen und die Ressourcen innerhalb Ihres Partnernetzwerks zu kontrollieren. Gluu, das US-amerikanische Unternehmen hinter Gluu Server und Partner der DAASI International, bietet die zentralen Funktionen für Authentifizierung und Autorisierung von Gluu Server gebündelt als Open-Source-Variante mit Namen Janssen an. Sowohl Gluu Server als auch Janssen können durch Zusatztools ergänzt werden. Basierend auf den Protokollen SAML, OpenID Connect und OAuth2 ist es möglich verschiedenste Anwendungen anzubinden. Durch Features wie Multi-Faktor-Authentifizierung (MFA), Social-Login, Identity-Management-APIs und Single-Sign-On für alle Anwendungen – auch über die Grenzen der genannten Protokolle hinweg – lassen sich Sicherheit und User Experience signifikant verbessern.



Mit OpenLDAP gibt es eine Open-Source-Lösung für die heute standardmäßige zentrale Benutzerverwaltung. OpenLDAP integriert den IETF-Standard LDAP (Lightweight Directory Access Protocol) und dient als Bezugssystem für andere Implementierungen. OpenLDAP ist eine der leistungsfähigsten LDAP-Implementierungen. Sie kann sich selbstständig an die Leistungsfähigkeit vorhandener Hardware anpassen und verleiht so jeder IT-Infrastruktur mehr Stabilität. OpenLDAP ist ein Open-Source-Gemeinschaftsprojekt, und wird von Entwickler*innen auf der ganzen Welt stetig verbessert, um das Ziel einer voll ausgestatteten Open-Source-LDAP-Suite zu erreichen. Die derzeit stabilste OpenLDAP-Distribution kommt aus dem Hause Symas, 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 (Lightning Memory-Mapped Database) oder dem Hashverfahren PBKDF2 zeitgemäße Technologien für bessere Performanz und höhere Sicherheit an.



privacyIDEA ist ein System für Multi-Faktor-Authentifizierung (MFA), das die Firma NetKnights entwickelt. Die Lösung erhöht den Schutz empfindlicher Daten durch mehr als einen Faktor bei der Authentifizierung erheblich. Der modulare Aufbau erlaubt eine individuelle Anpassung gemäß Kundenwunsch sowie beliebige Erweiterungen. Da die Software sowohl Mandanten- als auch Multi-Instanz-fähig ist, eignet sie sich für Organisationen jeder Größenordnung. Die Schnittstellen, die privacyIDEA für die Kommunikation benutzt, sind moderne REST-Schnittstellen, sodass eine einfache und nahtlose Integration in bestehende IT-Landschaften möglich ist. Bereits jetzt unterstützt privacyIDEA für MFA die meisten gängigen Tokens. Durch stetige Weiterentwicklung werden zunehmend mehr Tokenarten unterstützt und regelmäßig kommen neue Verfahren hinzu. Auf diese Weise kann privacyIDEA höchste Sicherheit bei maximal spezialisierten Authentifizierungsworkflows gewährleisten.

didmos (DAASI IdM with Open Source) ist das IAM-Framework von DAASI International. Seine Stärke liegt in der modularen Form: Es besteht aus insgesamt sechs anpassbaren und über Plugin-Schnittstellen erweiterbaren Open-Source-Modulen, die alle aufeinander abgestimmt sind und sich hervorragend ergänzen. Zusammen bilden sie ein umfassendes, leistungsstarkes und standardkonformes IAM-System, in dessen Zentrum ein mit OpenLDAP implementiertes Metadirectory steht. So ermöglicht uns didmos, individuell auf Kundenwünsche und spezielle Anforderungen einzugehen. Alle Komponenten sind unabhängig voneinander einsetzbar und können einzeln in bestehende IT-Infrastruktur integriert werden.

Das IAM-Framework DIDMOS

Das LDAP User Interface, kurz LUI, bildet den Kern von didmos und besteht aus drei Elementen: Einer Frontend-Komponente zur Verwaltung von Benutzer*innen oder für deren Selbstadministration, einem Backend für Businesslogik und Workflow-Engine sowie einem Metadirectory als Persistenzschicht. In das LUI-Backend lassen sich beliebige weitere Module integrieren, wie der DecisionPoint oder kundenspezifische Module mit eigener API. Durch die Unterstützung des internationalen Standards SCIMv2 zur Verteilung von Identitäten in der Cloud, kann das Backend universell eingesetzt werden. LUI ist auf vielen Ebenen individualisierbar und lässt sich ganz einfach an Ihr Corporate Design anpassen.

Der didmos Authenticator ist eine universell einsetzbare Authentifizierungskomponente, die durch ihren modularen Aufbau an individuelle Anforderungen innerhalb jeder SSO-Umgebung angepasst werden kann. Benutzer*innen können sich sowohl über lokale als auch über externe Accounts, z. B. via Social-Login, anmelden. Dies ist durch die Einbindung der Protokolle SAML und OpenID Connect möglich. So können Benutzer*innen 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 didmos Authenticator mit der Open-Source-Lösung privacyIDEA unseres Partners NetKnights verbinden.

Der didmos Pwd Synchroniser synchronisiert eventbasiert Passwortänderungen 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.

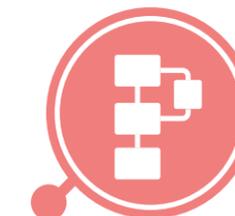
Das Modul ETL Flow (Extract, Transform, Load, Workflow) sorgt für die Extrahierung von Daten aus verschiedenen Quellen – etwa aus ERP-, SAP-, XML- oder SQL-Datenbanken – die schließlich in das zentrale Metadirectory synchronisiert werden. Entscheidende Prozesse sind dabei die Identifizierung von Identitäten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

Der didmos Provisioner ermöglicht eine Übertragung von Identitätsinformationen in angeschlossene Zielsysteme in Echtzeit. Relevante Änderungen werden als JSON-Dokument in das Queuing-System RabbitMQ geschrieben und darauf 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 oder eigene Konnektoren zur Anbindung proprietärer Systeme eingebunden werden können.

didmos Core ermöglicht die Verwaltung von Objekten, Benutzer*innen und Gruppen. Das Softwaremodul ist in Python geschrieben und greift dabei auf das Django-Framework zurück. Dieses erlaubt Entwickler*innen ein teilweise automatisiertes Schreiben von App-Codes, was den Entwicklungsprozess stark vereinfacht. Core stellt SCIM-v2-Endpunkte und Endpunkte für die Verwaltung und Abfrage von Zugriffskontrollinformationen sowie die Implementierung mehrstufiger Workflows zur Verfügung, die als REST-Aufrufe umgesetzt wurden. Ein Metadirectory in Form eines LDAP-Servers fungiert als Daten-Backend. Damit ist didmos Core auch eine Webservice-Schnittstelle, die es ermöglicht, in einen LDAP-Server zu schreiben und ihn auszulesen. So können zusätzlich Business-Logiken implementiert werden. Da SCIM viel einfacher zu implementieren ist als LDAP, können über didmos Core auch schlanke JavaScript-basierte Frontends auf LDAP-Daten zugreifen.



ETL FLOW



PROVISIONER



CORE



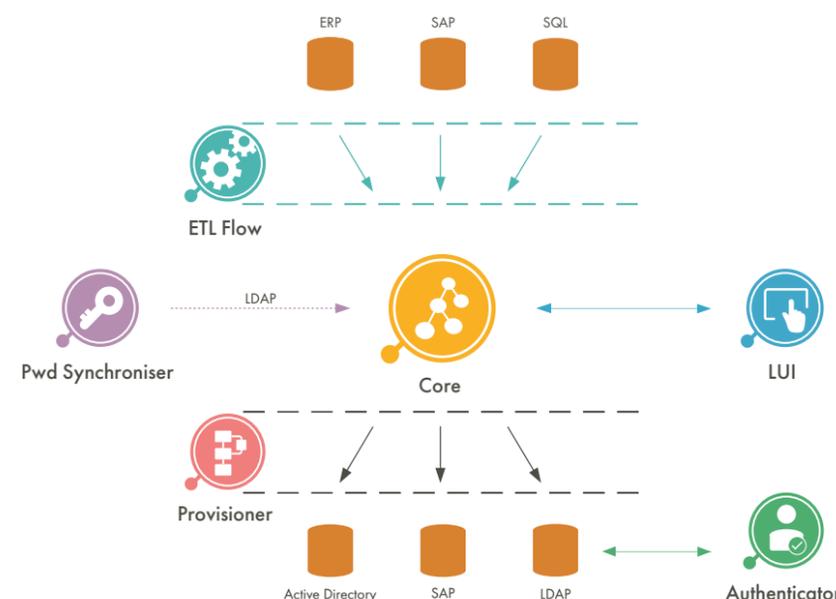
LUI



AUTHENTICATOR



PWD SYNCHRONISER





Unsere Produkte

SSO-Technologien

SINGLE-SIGN-ON

Single-Sign-On (SSO) steht für Authentifizierungsverfahren, die es Nutzer*innen erlauben, Zugriff auf verschiedene Anwendungen mit lediglich einem einmaligen Login zu erhalten. Möglich wird dies, indem die Authentifizierung der Anwendungen an eine zentrale Komponente – den Identity Provider (IdP) – ausgelagert wird.

Die DAASI International vertreibt und unterstützt neben Gluu drei weitere Open-Source-Produkte, die sich im SSO-Bereich etabliert haben.

SHIBBOLETH

Shibboleth ermöglicht föderierte Authentifizierung und Autorisierung für Webanwendungen. Diese Lösung wird vor allem in Verbänden von Hochschulen, Behörden und Großunternehmen eingesetzt und basiert auf dem SAML-Standard. Shibboleth bietet hierzu zwei Komponenten an:

1. Mit dem Shibboleth Identity Provider (IDP) lässt sich ein zentraler Login realisieren, an den die Dienste der eigenen Organisation oder die einer ganzen Föderation angeschlossen werden können.
2. Mit dem Shibboleth Service Provider (SP) lassen sich Webanwendungen schützen, sodass diese das komplexe SAML-Protokoll nicht unterstützen müssen.

Auf Wunsch erweitert die DAASI International Shibboleth auch über dessen Standardfunktionalität hinaus, etwa mithilfe von Plugins zur Unterstützung einer Multi-Faktor-Authentifizierung, oder durch neue, in der Community entstandene Module zur Unterstützung von OpenID Connect.

SIMPLESAMLPHP

Ursprünglich entwickelt von Mitarbeiter*innen des norwegischen Forschungsnetzes Uninett, wird SimpleSAMLphp heute von einer großen Open-Source-Community getragen. Wie Shibboleth ermöglicht SimpleSAMLphp Single-Sign-On basierend auf dem XML-Standard SAML. „Out of the box“ wird hier ein vergleichsweise limitiertes Set an Funktionen geboten, jedoch lassen sich Konfigurationsänderungen damit deutlich einfacher umsetzen. Daher ist SimpleSAMLphp für „Proofs of Concept“ häufig die beste Wahl.

Darüber hinaus basiert die Software vollständig auf PHP, was die Einbindung von PHP-Anwendungen erleichtert.

Die DAASI International passt auch SimpleSAMLphp gerne individuell an Ihre Bedürfnisse an.

SATOSA

Das Authentifizierungstool Satosa ähnelt Shibboleth auf den ersten Blick sehr. Tatsächlich ist Satosa aber ein Proxy, der zwischen einem Dienst und einem Identity-Provider geschaltet wird. Dieser Proxy besteht aus zwei Komponenten, die jeweils mit dem Dienst oder dem Identity Provider sowie untereinander kommunizieren. Satosa ermöglicht es, die Kommunikation zwischen Dienst und Identity-Provider transparent weiterzuleiten oder zu modifizieren. Dabei können Attribute geändert oder von zusätzlichen Datenbanken abgefragt werden. Sogar das Authentifizierungsprotokoll kann gewechselt werden, wodurch Kommunikation teilweise erst ermöglicht wird.

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

Übrigens bildet Satosa die Grundlage des didmos Authenticator von DAASI International.

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

SCHULUNGEN

Als Botschafterin für IAM mit Open-Source-Technologie vermittelt die DAASI International ihr Wissen auch gerne weiter. Unsere IAM-Experten schulen Ihr Personal zu Themen wie LDAP, SAML, OIDC und OAuth2 sowie zu unseren Open-Source-Lösungen. Für eine zielgerechte Wissensvermittlung passen wir das Präsentationsmaterial individuell an Ihre Bedürfnisse 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 die für Sie individuell entwickelten Lösungen sowie für alle angebotenen Standardprodukte. Gerne beantworten wir Ihnen 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

Im Mittelpunkt des Projekts der GESIS – Leibniz-Institut für Sozialwissenschaften stand deren Anbindung an die DFN-AAI und der gleichzeitige Aufbau einer eigenen Authentifizierungs-Infrastruktur.

DIE SPEZIFIKATIONEN

Weitere Ziele waren, neben der Einführung eines Single-Sign-On, eigene Angebote auch den Benutzer*innen anderer Organisationen bereitzustellen, sowie den eigenen Nutzer*innen die Angebote der anderen Mitglieder der DFN-AAI zur Verfügung zu stellen.

HERAUSFORDERUNGEN

Ermöglichung eines Single-Sign-On für die GESIS-Mitarbeiter*innen bei der Nutzung ihrer Anwendungen und Anbindung an die DFN-AAI.



UNSER BEITRAG

Es wurde ein Shibboleth Identity Provider aufgebaut, welcher seine Daten aus einem OpenLDAP-basierten Verzeichnisdienst bezieht. Durch eine Anbindung an das Active Directory konnte eine automatische Befüllung der Benutzerinformationen in den Verzeichnisdienst erreicht werden, sodass nun auch Passwortänderungen der Benutzer direkt synchronisiert werden.

DAS PROJEKT

Das Max-Planck-Institut für Festkörperforschung beauftragte den Aufbau eines Active Directory (AD) mit dem Ziel, den bisherigen OpenLDAP-Server weiterhin als primäres System für Benutzer*innen und Gruppenmitgliedschaften verwenden zu können.

DIE SPEZIFIKATIONEN

Benutzer*innen sollten ihr Passwort für alle Anwendungen und Systeme am Arbeitsplatzrechner ändern können. Hierzu wurde eine Lösung konzipiert, die Passwörter aus dem AD in das OpenLDAP-Verzeichnis synchronisiert.

HERAUSFORDERUNGEN

An diesen OpenLDAP-Server war bislang ein als NT4 Domain Controller konfigurierter Samba-Server angeschlossen, den es durch besagtes Active Directory abzulösen galt.



UNSER BEITRAG

Das verwendete didmos-Modul ETL Flow wurde so konfiguriert, dass eine vollständige Synchronisierung der Daten bei Bedarf jederzeit erneut durchgeführt werden kann, sollten die Zieldaten fehlerhaft sein. Als dauerhafte Lösung sorgt der didmos Provisioner für sekundenschnelles Auslesen und übermittelt Attributänderungen von Benutzer*innen aus dem OpenLDAP-Server in das AD, was eine permanente Aktualisierung ermöglicht.

DAS PROJEKT

Im Rahmen des IT-Investitionsprogramms der Bundesregierung sollte das Dienstleistungszentrum für Informationstechnik im Geschäftsbereich des BMVBS (DLZ-IT BMVBS) ihre auf Novell-Software basierte Verzeichnisdienst-Infrastruktur nach Open-Source migrieren.

DIE SPEZIFIKATIONEN

Gemäß den Anforderungen sollte die Lösung möglichst über dieselben Funktionen wie die des abzulösenden Systems verfügen, wie etwa die Möglichkeit zur Vergabe von Berechtigungen oder Passwortsynchronisierung. Gewünscht waren außerdem Single-Sign-On und die Implementierung von automatischen Prozessabläufen.

HERAUSFORDERUNGEN

Die Infrastruktur bestand aus einem zentralen Meta-Verzeichnis, in das Daten aus ADs von über 60 dezentralen Dienststellen sowie aus einem weiteren BMVBS-Verzeichnisdienst synchronisiert wurden. Diese anspruchsvolle Infrastruktur galt es im Produktivbetrieb umzustellen.

Bundesministerium für
Verkehr, Bau &
Stadtentwicklung (BMVBS)

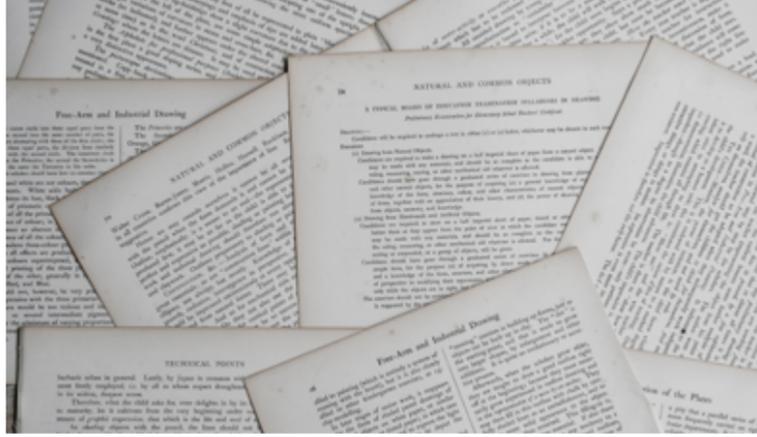
UNSER BEITRAG

Die Lösung konnte nicht nur alle Funktionalitäten des bisherigen Systems abbilden (u. a. ein sehr flexibles und komplexes Berechtigungssystem sowie geschützte Synchronisierung von Passwörtern), sondern auch neue Eigenschaften einbringen, wie föderiertes Single-Sign-On und ein interaktiver Genehmigungsworkflow für die Erteilung von Zugriffsberechtigungen.

Unsere Kunden

WEITERE REFERENZEN





Die Zukunft der Geisteswissenschaften **DIGITAL HUMANITIES**

In den „digitalen Geisteswissenschaften“, den sogenannten Digital Humanities (DH), werden geisteswissenschaftliche Forschungsansätze mit dem Einsatz von Algorithmen kombiniert. Dabei werden Methoden und Tools der modernen Informationstechnologie verwendet, um in den einzelnen Disziplinen wie der Linguistik, der Archäologie oder den Geschichts- und Kulturwissenschaften neue Erkenntnisse zu gewinnen und innovative Forschungsfragen beantworten zu können. Zu den dabei verwendeten IT-Komponenten gehören unter anderem Anwendungen für Langzeitarchivierung, kollaboratives Arbeiten, Visualisierung, Statistik, komplexe Suchalgorithmen und Text Mining.

Die systematische Verwendung und Auswertung von digitalen Ressourcen sowie die weltweite Vernetzung von Wissenschaftler*innen ermöglichen zudem neue Kollaborationsformen und Arbeitsweisen.

Die DAASI International bietet verschiedene Tools für Forschung und Lehre an, die Wissenschaftler*innen und Dozent*innen bei ihrer täglichen Arbeit unterstützen können.

Mehr Erkenntnisse gewinnen mit **DH-TOOLS**

FELDPARTITUR

Die Feldpartitur ist ein digitales Tool zur Video- und Film-analyse, das bisher vor allem in der Sozialforschung zum Einsatz kommt. Die Software erlaubt es, zu jeder Sequenz eines Videos Informationen in Form von Text (z. B. Beschreibungen), Schlagwörtern, Transkriptionen oder visuellen Symbolen manuell zu editieren, ähnlich wie bei einer Musikpartitur. Das Tool entstand im Rahmen einer Forschungsarbeit von Frau Dr. Christine Moritz und wird von ihr durch die Feldpartitur GmbH vertrieben, während die DAASI International technische Dienstleistungen wie Installation und Weiterentwicklung sowie den Support der Software übernimmt.

CONEDAKOR

Die innovative Datenbank ConedaKOR ist besonders geeignet, Daten, insbesondere Bilder, in einer Netzstruktur semantisch zu annotieren. Unter Verwendung der sogenannten Graphdatenbank-Technologie, können Informationen einfacher, detaillierter und schneller verwaltet werden. ConedaKOR verfügt über attraktive Funktionen, die das Informationsmanagement erheblich erleichtern. Wissenschaftliche Institutionen aus aller Welt vertrauen bereits auf ConedaKOR und setzen schon seit Jahren auf diese Art der Medienverwaltung.

Die DAASI International bietet ConedaKOR als Software as a Service an, damit sich Forscher*innen auf ihre Arbeit konzentrieren können und sich nicht um betriebliche Fragen kümmern müssen.

HYPERIMAGE

Die virtuelle Forschungsumgebung HyperImage ermöglicht die Verknüpfung von Anmerkungen und Metadaten mit Bildern, Bilddetails und Texten. Dadurch kann ohne textuellen Bezug auf beliebige Daten verwiesen werden. Es handelt sich somit auch um „vorsprachliche“ bildhafte Fußnoten, mit denen das Konzept des Hypertextes auf Bilder angewendet wird. Initiiert wurde das Projekt von Prof. Martin Warnke an der Leuphana Universität Lüneburg. Die DAASI International unterstützt die Leuphana Universität bei der kontinuierlichen Weiterentwicklung und Verbesserung von HyperImage.



LEISTUNGEN im Bereich der Digital Humanities

Die DAASI International hat es sich zur Aufgabe gemacht, Geisteswissenschaftler*innen bei der Verwendung von DH-Methoden umfassend zu unterstützen und so Anwender*innen und Entwickler*innen von DH-Tools zu fördern. Als einer der wenigen privatwirtschaftlichen IT-Anbieter für Digital Humanities in Europa bietet DAASI International ein umfassendes Leistungsspektrum auf technischer sowie auf Projektebene an.

TECHNISCHE SERVICES

Wir entwickeln und implementieren innovative Authentication and Authorisation Infrastructures (AAIs) sowie Datenbanken und Visualisierungstools und konzipieren für Sie nachhaltige Betriebsmodelle.

SERVICES AUF PROJEKTEBENE

Auf Wunsch stellen wir Ihnen unser Know-How im Bereich Projektmanagement zur Verfügung und unterstützen Sie bei der Erstellung des Forschungsantrages sowie bei der Suche nach kommerziellen Kooperationspartnern für Ihr Forschungsprojekt.

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, Verknüpfung von bisher getrennten Aktivitäten und über generische Dienste der technischen Infrastruktur. Vorhandene digitale Ressourcen sowie Anwendungen und Erkenntnisse werden unabhängig von der Disziplin gemeinsam genutzt und miteinander verknüpft. Neben Aufbau und Betrieb der AAI, der Integration neuer Technologien und der Entwicklung von nachhaltigen 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 ist. 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.

PROJEKTE im Bereich der Digital Humanities

DARIAHDOCS

DARIAHdocs ist ein Dienst der DAASI International für die europäische geisteswissenschaftliche Forschungsinfrastruktur DARIAH-EU. Dieser ermöglicht es, Dokumente mit Kolleg*innen gemeinsam und zur selben Zeit zu bearbeiten, ohne die Inhalte an einen Cloud-Provider preisgeben zu müssen. DARIAHdocs für kollaboratives Arbeiten basiert auf Collabora, einer kommerziell unterstützten Version des Open-Source-Produkts Libre Office Online. Die DAASI International übernimmt das DSGVO-konforme Hosting sowie den nachhaltigen Betrieb von DARIAHdocs und sorgt so für die Sicherheit der sensiblen Forschungsdaten.



Als Spin-off von Forschungsprojekten zu X.500 und LDAP, die vom Bundesministerium für Bildung und Forschung (BMBF) gefördert wurden, war die DAASI International von Anfang an mit der Forschung verbunden und pflegt diese Beziehung bis heute. Auch als privates Unternehmen beteiligt sie sich mit ihrer Forschungsabteilung nach wie vor an innovativen Projekten.

Mit der Forschungsbeteiligung verdient die DAASI International kein Geld. Jedoch ist die Zeit, die wir darauf verwenden, uns mit neuesten Internettechnologien zu beschäftigen sowie der Kontakt zu den besten Köpfen im Bereich der Forschung zu Authentication and Authorisation Infrastructures (AAI) für uns sehr wertvoll. Die daraus resultierende Erfahrung, das Know-How und die Kontakte bringen unser Unternehmen voran und sind deshalb ein klares Asset.

Wir engagieren uns in der **FORSCHUNG**

Die DAASI International wirkte in besonderem Umfang an Projekten im Rahmen der D-Grid-Initiative sowie weiteren Projekten in den Bereichen Digital Humanities und Forschungsinfrastruktur mit. Besonders wichtige Projekte waren hierbei die vom BMBF geförderten Projekte TextGrid und DARIAH. Darin war die DAASI International jeweils an allen Projekt-Phasen beteiligt und dabei allem voran für den Aufbau einer international anschlussfähigen AAI für geisteswissenschaftliche Forschungsumgebungen und Forschungsinfrastrukturen zuständig. In DARIAH hat die DAASI International zudem an den Nachhaltigkeitsbestrebungen mitgewirkt und die sogenannte DARIAH eInfrastructure Service Unit (DeISU) konzipiert und mit aufgebaut.

Von besonderer Bedeutung war die Beteiligung an beiden Phasen des EU-Projekts „Authentication and Authorisation for Research Collaboration“ (AARC), in dem Blaupausen für moderne AAI erforscht und spezifiziert wurden, an die sich die meisten Forschungsinfrastrukturen, einschließlich so exponierte, wie die des CERN, halten. Den in AARC gewonnenen Wissensvorsprung konnte die DAASI International bereits in mehreren großen Projekten erfolgreich einsetzen.

Schließlich führt die DAASI International auch eigene Grundlagenforschung zu AAI und Föderationen durch und betreut Abschlussarbeiten von Universitäten und Hochschulen – für uns ein hervorragender Weg, junge Talente für unser Unternehmen zu gewinnen.



Diese Broschüre wurde auf 100% Recyclingpapier gedruckt



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