Beitragsaufruf

Von der Wallet zum Vertrauensökosystem: Verifizierbare Daten für Menschen, Organisationen & KI

Über die authenticon 2027

Die authenticon ist die Konferenz für Vertrauen in der digitalen Gesellschaft. Sie bringt Menschen aus Wirtschaft, Verwaltung, Wissenschaft und Politik zusammen, um darüber zu diskutieren, wie Vertrauen in digitalen Prozessen hergestellt werden kann – technisch, organisatorisch und gesellschaftlich.

Nach dem Start der europäischen digitalen Brieftasche (EUDI-Wallet) richtet sich der Blick 2027 auf die Praxis: Wie werden Wallets und digitale Nachweise in bestehende Geschäftsprozesse und Verwaltungsabläufe integriert? Wie werden Organisationen technisch und organisatorisch befähigt, Nachweise auszustellen und zu prüfen? Wie entstehen aus einzelnen Anwendungen tragfähige Vertrauensökosysteme?

Mit neuen technischen Möglichkeiten verändern sich zugleich die Erfahrungen der Menschen, die diese Systeme nutzen oder mit ihnen arbeiten. Für Nutzende stellt sich die Frage, ob digitale Nachweise Prozesse tatsächlich vereinfachen oder neue Hürden schaffen. Mitarbeitende in Behörden und Unternehmen müssen neue Abläufe verstehen, Entscheidungen erklären, Fehlerfälle bearbeiten und Nutzende unterstützen. Fragen nach Benutzerfreundlichkeit, Barrierefreiheit, Transparenz und Datensparsamkeit gehören deshalb ebenso zur Diskussion wie die technische Architektur und die Regulierung.

Gleichzeitig entstehen neue Formen digitaler Interaktion. KI-Agenten können selbstständig Informationen beschaffen, Entscheidungen vorbereiten oder Transaktionen ausführen. Damit wird die Frage dringlicher, wer oder was in digitalen Prozessen eigentlich handelt: Wie lässt sich nachweisen, für wen ein Agent tätig ist? Welche Befugnisse wurden ihm übertragen? Wie können solche Befugnisse geprüft, eingeschränkt oder widerrufen werden? Und welche Nachweise brauchen wir, um die Eigenschaften von KI-Systemen selbst verlässlich beurteilen zu können?

Auch die notwendige Vertrauensinfrastruktur hinter digitalen Nachweisen rückt stärker in den Vordergrund. Trust Lists, Register, Rulebooks, Standards, Intermediäre und gemein same technische Komponenten entscheiden darüber, ob Vertrauen über einzelne Organi sationen und Anwendungsfälle hinaus funktioniert. Gleichzeitig stellt sich die Frage, wie solche Infrastrukturen gestaltet werden müssen, damit sie offen, interoperabel, wirtschaftlich tragfähig und für die Beteiligten nachvollziehbar bleiben.

Welche Beiträge suchen wir?

Uns interessieren keine Produktpräsentationen und Hochglanzfolien, sondern ein konstruktiver und offener Austausch. Besonders willkommen sind Beiträge zu:

- Erfahrungen aus realen Anwendungen und laufenden Projekten
- belastbare Erkenntnisse aus Pilotierung, Einführung und Betrieb
- Fallstudien und sektorübergreifende Erfahrungen
- Beiträge, die Zielkonflikte, Hindernisse oder gescheiterte Ansätze offen diskutieren
- Perspektiven von Nutzenden und Mitarbeitenden
- Beiträge zu offenen Forschungs- und Gestaltungsfragen

Themen

Die folgenden Themenfelder dienen als Orientierung. Beiträge zu angrenzenden Fragestellungen sind ausdrücklich willkommen.

1. Wallets und digitale Nachweise in der Praxis

Mit dem Rollout der EUDI-Wallet beginnt die eigentliche Arbeit häufig erst. Wir interessieren uns für Erfahrungen aus der Einführung und dem Betrieb von wallet-basierten Anwendungen.

- Onboarding und technische Befähigung von Ausstellenden und Prüfenden
- Integration in Fachverfahren, Unternehmenssoftware und bestehende Nutzerkonten
- Gestaltung, Ausstellung, Prüfung und Widerruf digitaler Nachweise
- Customer Journeys, Benutzerfreundlichkeit, Barrierefreiheit und Support
- Auswirkungen auf Mitarbeitende, interne Abläufe und Change Management
- Nutzen, Kosten, Hindernisse und Erfahrungen aus konkreten Anwendungsfällen

Themenkooperation mit dem NEGZ: Mit dem NEGZ – Kompetenznetzwerk Digitale Verwaltung planen wir einen Schwerpunkt zur EUDI-Wallet in der öffentlichen Verwaltung. Besonders willkommen sind Beiträge zu konkreten Anwendungen, die Erfahrungen von Behörden und Beschäftigten sowie die Perspektive von Bürgerinnen und Bürgern einbringen. Vorgesehen sind Vorträge und ein interaktives Format.

2. Organisationen, Business Wallets und digitale Vertretung

Digitale Identität betrifft nicht nur natürliche Personen. Unternehmen, Behörden und andere Organisationen müssen selbst digital handlungsfähig sein und nachweisen können, wer in ihrem Namen handeln darf.

- European Business Wallet und andere Ansätze für digitale Organisationsidentitäten
- Standards und Umsetzungsvarianten für Business Wallets
- Rollen, Berechtigungen, Vollmachten und Vertretungsregelungen
- Integration in IAM-, Unternehmens- und Verwaltungsprozesse
- Open Source, gemeinsame Infrastrukturkomponenten und Betreibermodelle
- grenzüberschreitende Nutzung und Zusammenspiel mit Datenräumen und anderen Infrastrukturen

3. Vertrauenswürdige KI und digitale Agenten

Mit KI-Agenten treten neue Akteure in digitale Prozesse ein. Sie können im Auftrag von Menschen oder Organisationen handeln, ohne dass bei jeder einzelnen Handlung ein Mensch unmittelbar beteiligt ist.

- prüfbare Identität von KI-Agenten und Nachweis ihrer Auftraggeber
- Delegation, Begrenzung und Widerruf von Handlungsspielräumen
- Rolle von Business Wallets und verifizierbaren Nachweisen für Agenten
- Nachweise, Zertifizierungen und Herkunftsinformationen für KI-Systeme und Inhalte
- vertrauenswürdige Interaktionen zwischen Agenten, Menschen und Organisationen
- neue Angriffs-, Manipulations- und Missbrauchsmöglichkeiten durch autonome Systeme

4. Vertrauensökosysteme aufbauen und skalieren

Digitale Nachweise entfalten ihren Nutzen erst dann, wenn viele Organisationen auf gemeinsame Regeln und Infrastrukturen vertrauen können. Besonders spannend sind Beiträge, die nicht nur beschreiben, wie Governance formal aussehen sollte, sondern auch zeigen, welche Regeln und Anreize in der Praxis tatsächlich funktionieren.

- Governance, Rulebooks und Trust Management
- Trust Lists, Register und gemeinsame Vertrauensinfrastrukturen
- Rollen, Verantwortlichkeiten und Intermediäre in Vertrauensökosystemen
- Anreizmechanismen, Geschäftsmodelle und Verteilung von Kosten und Nutzen
- Standardisierung sowie technische und semantische Interoperabilität
- internationale Interoperabilität und grenzüberschreitende Nachweise

5. Digitale Souveränität, Privatsphäre und Missbrauchspotenziale

Mehr überprüfbare Daten bringen nicht nur Vorteile. Digitale Nachweise können Daten sparsamkeit erleichtern, aber auch neue Formen der Überidentifikation, Überwachung und Abhängigkeit schaffen. Von besonderem Interesse ist die Perspektive der Betroffenen: Welche Daten werden tatsächlich benötigt und können Menschen nachvollziehen, wer welche Informationen zu welchem Zweck erhält? Und wie verhindern wir, dass aus einer Infrastruktur für digitales Vertrauen eine Infrastruktur für unnötige Kontrolle wird?

- Datensparsamkeit, selektive Offenlegung, Pseudonymität und anonyme Nutzung
- Altersverifikation und Jugendschutz zwischen Wirksamkeit und Überwachung
- Schutz vor Profilbildung und Transparenz über die weitere Nutzung von Daten
- verständliche Freigabe- und Entscheidungsprozesse sowie Möglichkeiten zum Widerspruch
- Inklusion und Alternativen für Menschen, die digitale Verfahren nicht nutzen können oder wollen
- Deepfakes, Identitätsdiebstahl, Betrug und die Grenzen technischer Vertrauensmechanismen
- Open Source Wallets und offene Vertrauens-Infrastrukturen, souveräne Bereitstellung und Auslieferkanäle

6. Zukunft des digitalen Vertrauens

Neben den aktuellen Herausforderungen möchten wir auf der authenticon 2027 auch Raum für Fragen schaffen, die in die Zukunft weisen.

Wie verändert sich die digitale Identität, wenn autonome Agenten selbstverständlich werden? Welche Rolle werden nationale elektronische Identitäten in zehn Jahren noch spielen? Wie interagieren Menschen, Organisationen und Maschinen künftig miteinander? Und welche Formen von Vertrauen brauchen wir in einer digitalen Gesellschaft, die heute erst in den Anfängen sichtbar sind?

Für solche Fragen planen wir ein eigenes Format mit Impulsvorträgen und einer gemeinsamen Diskussion. Beiträge dazu dürfen ausdrücklich spekulativer sein als im übrigen Programm, sollten jedoch eine konkrete These oder Fragestellung enthalten.

Einreichung

Beitragsformate

Bitte geben Sie an, welches Format Ihr Beitrag haben soll:

- **Vortrag:** Dauer 30 min, im Regelfall 20 min Präsentation + 10 min Diskussion. Bei interaktiven Vorträgen können die 30 min auch anders aufgeteilt werden.
- **Workshop:** Interaktives Format mit einer Dauer von 90 oder 45 min. Die Teilnehmerzahl ist auf 30 Personen beschränkt.
- **Impulsvortrag:** Kurzbeitrag mit einer zugespitzten These oder Frage zur Zukunft digitaler Identitäten und des digitalen Vertrauens. 10 min Vortrag + 20 min Diskussion.
- **Lightning-Talk:** Kurzvortrag mit 5 min Dauer und maximal 5 Folien.
- **Demo:** 15 min Live-Demonstration einer wallet-basierten Anwendung (Ausstellung oder Prüfung eines Nachweises) + 5 min Fragen. Voraussetzung: lauffähige Umsetzung, keine Produktpräsentation.

Hinweise zu Beitragsvorschlägen

Regeln für Beitragsvorschläge:

- Alle Beiträge müssen auf Deutsch sein.
- Eigene Produkte und Leistungen dürfen im Kontext konkreter Projekterfahrungen und technischer Ansätze neutral genannt werden. Werbliche und marketing-orientierte Beiträge sind unzulässig.
- Beiträge können auch kritisch und kontrovers sein, solange die Darstellung sachorientiert und konstruktiv ist. Für Polemik gibt's das Heise-Forum! ;-)

Wenden Sie sich bei Fragen gern an uns per Email: einreichung@authenticon.io.

Einreichungsformat und -frist

Titel, gewünschtes Format, Abstract (max. 1.500 Zeichen), Referierende mit Organisation und Rolle, Zielgruppe/Vorkenntnisse, Angabe, ob eine Live-Demo enthalten ist, ggf. Zuordnung zu einem Themenschwerpunkt.
Einreichung per E-Mail an einreichung@authenticon.io.
Die Frist für die Einreichung von Beitragsvorschlägen ist der **04.12.2026**.

Annahme und Vorbereitung der Beiträge

- Die Entscheidung über die Annahme von Beiträgen trifft das Programmkomitee unter Abwägung der Attraktivität des Themas für das Publikum, der thematischen Breite des Programms sowie der Einhaltung der genannten Hinweise zu Beitragsvorschlägen.
- Die Rückmeldung zur Annahme oder Ablehnung von Beiträgen erfolgt bis spätestens zum **18.12.2026**.
- Die vorläufigen Präsentationsfolien müssen bis spätestens **01.03.2027** vorliegen. Das Programmkomitee behält sich das Recht vor, Änderungen an Beiträgen zu verlangen, wenn diese den genannten Regeln nicht entsprechen.

Programmkomitee

- Prof. Jürgen Anke, HTW Dresden
- Ricardo Bochnia, HTW Dresden
- Benjamin Burde, Consultant
- Dr. Gunnar Hempel, HTW Dresden
- Sandra Kostic, Fraunhofer AISEC
- Dr. Michael Kubach, Fraunhofer IAO
- Daniel Richter, HTW Dresden
- Lilly Schmidt, Common Codes GmbH / SPRIND
- Prof. Johannes Schönrich, Technische Hochschule Augsburg / Fraunhofer FIT
- Dr. Carsten Stöcker, Spherity GmbH
- Prof. Jan Sürmeli, Universität Potsdam / FZI Forschungszentrum Informatik

Kontakt

authenticon.io

info@authenticon.io

linkedin.com/company/authenticon/