

TeleTrust-Informationstag "Blockchain"

Berlin, 27.06.2018

Personenzertifikate per Blockchain organisieren

Dr. Christian Baumann, AustriaPro/WKO

Inhalt

- AustriaPro
- Personenzertifikate auf der Blockchain
 - Definition
 - Status, Problemstellung
 - Lösungsansatz, Details
 - Nutzen
 - Weitere potentielle Anwendungen
- Zusammenfassung, Ausblick

AustriaPro

- Standardisierungs- und Expertenplattform
 - Umfeld der WKO
 - Als Verein organisiert, ca. 70 Mitglieder
- Fachwissen für WKO sowie für UnternehmerInnen
- Zusammenarbeit mit Organisationen im In-/Ausland
 - Austrian Standards Institute, CEN (Europa), UN/CEFACT (international)
 - OCG, **TeleTrust.de** uvm.
- Arbeitskreise, Pilotprojekte, Veranstaltungen

AustriaPro – Arbeitskreis Blockchain

- Ziele/Inhalte
 - Information für Unternehmen
 - sinnvolle & sinnlose Einsatzgebiete
 - Chancen/Risiken
 - Nationale/Internationale Entwicklungen
 - **Online-Ratgeber**
 - Usecases
 - **Zertifizierungen**
 - Transport & Logistik
 - Blockchain-Lab
 - ...
 - Standardisierung
 - Mitarbeit an ON-AG 001 88 (Blockchain)
- Nicht-Ziele
 - Kryptowährungen, Finanzbereich

AustriaPro – Blockchain-Lab

- Aufbau/Betrieb unterschiedlicher Technologien
 - Basis „klassische“ Kryptowährungen
 - vgl. Bitcoin, Litecoin ...
 - Ethereum basierend (Smart Contracts)
 - Multichain Umgebung (Consortium Chains)
 - „Nicht-Blockchain“ Technologien: IOTA ...
 - Frameworks: Hyperledger ...
- Hands On, praktische Erfahrungen
- Basis für Entwicklungen
 - Integration / APIs
 - Smart Contracts
- Basis für Prototypsysteme & PoCs

Inhalt

- AustriaPro
- Personenzertifikate auf der Blockchain
 - Definition
 - Status, Problemstellung
 - Lösungsansatz, Details
 - Nutzen
 - Weitere potentielle Anwendungen
- Zusammenfassung, Ausblick

Definition

- Personenzertifizierung
 - Kompetenzen & Qualifikationen überprüfen
 - Übereinstimmung mit Zertifizierungsprogramm
 - Wissen & Können
- Personenzertifikate
 - (ÖNORM) EN ISO/IEC 17024
 - Personen im Produktions- und Dienstleistungssektor
 - Akkreditierte Zertifizierungsstellen (Ö: 12)
 - Zertifikate sind „öffentlich verfügbar“
 - gesetzliche Grundlage
 - (Aber auch DSGVO!)

Akkreditierung der Zertifizierungsstellen (Ö)

Es akkreditiert das BMDW (BM Digitalisierung und Wirtschaftsstandort)

Quality Austria - Trainings, Zertifizierungs und Begutachtungs GmbH	www.qualityaustria.com
SZA GmbH	www.sza.at
Wirtschaftskammer Österreich (WIFI)	www.wifi.at/Zertifizierungsstelle
Österreichische Gesellschaft für Zerstörungsfreie Prüfung	www.oegfzp.at
Bureau Veritas Austria GmbH	www.bureauveritas.at
TÜV SÜD Landesgesellschaft Österreich GmbH	www.tuev-sued.at
Österreichische Vereinigung für das Gas- und Wasserfach (ÖVGW)	www.ovgw.at
CIS - Certification & Information Security Services GmbH	www.cis-cert.com
SystemCERT Zertifizierungsgesellschaft m.b.H.	www.systemcert.at
Allgemeine Unfallversicherungsanstalt - Sicherheitstechnische Prüfstelle (STP)	www.auva.at
ImmoZert Zertifizierungsgesellschaft mbH	www.immozert.at
TÜV AUSTRIA CERT GMBH	www.tuev.at

<https://www.bmdw.gv.at/TechnikUndVermessung/Akkreditierung/Documents/certification%20bodies%20for%20persons.pdf> – 23.6.2018

Akkreditierung - Bescheid

Akkreditierung Austria

Akkreditierte Zertifizierungsstellen für Personen/ Accredited Certification Bodies for Persons*) gemäß / according to EN ISO/IEC 17024:2012

lfd. Nr. **3**

Wirtschaftskammer Österreich

Wiedner Hauptstraße 63
A-1045 Wien

Internet

www.wifi.at/Zertifizierungsstelle

Ident Nr.: 0907

**Zertifizierungsstelle des Wirtschaftsförderungsinstitutes der
Wirtschaftskammer Österreich**

Wiedner Hauptstraße 63, A-1045 Wien

Kontaktperson/
Contact

Mag. Dietmar Schönfuß

Telefon/ Mobile

0590900-5066

Fax

0590900-11 5066

Email

dietmar.schoenfuss@wko.at

Datum der Erstakkreditierung/
Initial accreditation Date

1996-02-24

Bescheid/ decree

GZ und Datum des Gültigkeitsbeginns siehe Beilage zum Bescheid (Akkreditierungsumfang)
accreditation decree number and granting/validity date see attachment (Scope of accreditation)

Akkreditierungsumfang/ Scope of accreditation

https://www.bmdw.gv.at/TechnikUndVermessung/Akkreditierung/Documents/AA_0907_17024_Zertifizierungsstelle_des_Wirtschaftsfoerderungsinstitutes_der_Wirtschaftskammer_Oesterreich.pdf

Akkreditierung – Umfang

Beilage zum Bescheid GZ.: BMWFV-92.331/0043-I/12/2016 Zertifizierungsstelle des Wirtschaftsförderungsinstitutes der Wirtschaftskammer Österreich_17024

Akkreditierungsumfang der Personenzertifizierungsstelle (EN ISO/IEC 17024:2012) Wirtschaftskammer Österreich

Zertifizierungsstelle des Wirtschaftsförderungsinstitutes der Wirtschaftskammer Österreich / (Ident.Nr.: 0907)

gültig ab: 21.11.2016

Nr.	Dokumentnummer der Norm bzw. SOP ¹⁾	Ausgabe	Titel der Norm bzw. SOP	Bemerkungen	PvO ²⁾
1	AD 2000-Merkblatt HP 3	2007-02	Schweißaufsicht, Schweißer	eingeschränkt auf Punkt 3 "Schweißer"	<input type="checkbox"/>
2	BGBl. II Nr. 451/2012	2012-12	Verordnung des Bundesministers für Gesundheit, mit der die Tiertransport-Ausbildungsverordnung geändert wird		<input type="checkbox"/>
3	BGBl. II Nr. 92/2008	2008-03	Verordnung der Bundesministerin für Gesundheit, Familie und Jugend über die Ausbildung von Personen, die Tiertransporte durchführen, Personen, die auf Sammelstellen mit Tieren umgehen, sowie Personen, die Tiertransportkontrollen durchführen (Tiertransport-Ausbildungsverordnung, TT-AusbVO)	Ausbildung von Personen, die Tiertransport durchführen, Personen die auf Sammelstellen mit Tieren umgehen, sowie Personen, die Tiertransportkontrollen durchführen	<input type="checkbox"/>
4	Interner Auditor	2007-04	Normatives Dokument des WIFI zur Zertifizierung von internen Auditoren		<input type="checkbox"/>
5	OENORM EN 12732	2013-07	Gasinfrastruktur - Schweißen an Rohrleitungen aus Stahl - Funktionale Anforderungen	eingeschränkt auf 10.2	<input type="checkbox"/>
6	OENORM EN 13067	2013-10	Kunststoffschweißpersonal - Anerkennungsprüfung von Schweißern - Thermoplastische		<input type="checkbox"/>
7	OENORM EN 14276-1	2011-05	Druckgeräte für Kälteanlagen und Wärmepumpen - Teil 1: Behälter - Allgemeine Anforderungen	eingeschränkt auf Anhang B	<input type="checkbox"/>
8	OENORM EN 14276-2	2011-04	Druckgeräte für Kälteanlagen und Wärmepumpen - Teil 2: Rohrleitungen - Allgemeine Anforderungen		<input type="checkbox"/>
9	OENORM EN 287-6	2010-02	Prüfung von Schweißern - Schmelzschweißen - Teil 6: Gusseisen		<input type="checkbox"/>
10	OENORM EN ISO 13585	2012-11	Hartlöten - Prüfung von Hartlötlern und Bedienern von Hartlöteinrichtungen (ISO 13585:2012)		<input type="checkbox"/>

Status in Österreich

- Mengengerüst (pro Jahr)
 - Erstzertifizierungen ca. 75.000
 - Verlängerungen ca. (25%) 18.000
- Landschaft
 - Viele Anbieter, viele Systeme
 - Proprietäre Systeme, Schnittstellen, GUIs
 - Nicht durchgängig digitalisiert und vernetzt
 - Papier, Kopie, Fax, Scan ...
 - Aufwändige Beauskunftung
 - Suche nach Personen, Zertifikaten ...
 - Validierung („Echtheitsprüfungen“)
 - Prüfungen erfolgen nicht durchgängig ...
 - => Ungültige Zertifikate (abgelaufen oder Falsifikate) werden nicht vollständig erkannt

Suche, Validierung ... heute ...

- ... zig Suchmasken ..."

Prüfung der Echtheit von uns ausgestellter Personenzertifikate

Sehr geehrte Kunden und Nutzer,

um die Sicherheit unserer Zertifikate zu gewährleisten, haben wir die Zertifikate präzise nach den Vorgaben der Akkreditierungsstelle ausgeführt.

Um die Echtheit eines Ihnen vorliegenden Zertifikates zu prüfen, vergleichen Sie dies zunächst mit dem links abgebildeten Musterzertifikat.

Die Überprüfung, ob das Zertifikat von uns ausgegeben wurde, können Sie durch Ausfüllen der Felder auf dem untenstehenden Formular vornehmen.

Aus datenschutzrechtlichen Gründen wird Ihre Anfrage nach Prüfung schriftlich beantwortet.

Echtheitsprüfung

Daten der anfragenden Organisation / Person:

Anrede*
Firma
Name*
Vorname*
Straße, Hausnummer*
PLZ, Ort*
E-Mail*

Informationen über die Zertifikate der TÜV AUSTRIA Gruppe

Neue Zertifikate mit QR-Code - FAQs

Personenzertifizierung Produktzertifizierung Systemzertifizierung

Abfrage-Formular

Personenzertifizierung - Suchkriterien

Vorname:
Vorname

Nachname:
Nachname

Zertifikat:
(Keine Auswahl)

Suchen

Zertifikats-Echtheitsprüfung

- Bitte füllen Sie alle mit einem * mit
- Anrede
 - Ihr Name*
 - Ihr Vorname*
 - Ihre Emailadresse*
 - Ihre Telefonnummer*
 - Name/Vorname auf dem Zertifikat*
 - Prüfungsdatum auf dem Zertifikat*
 - Prüfungsort auf Zertifikat*
 - Geburtsdatum auf Zertifikat*
 - Gültigkeitsbeginn auf Zertifikat*
 - Gültigkeitsende auf Zertifikat*
 - Zertifikat-Nr.*
 - Ihre Mitteilung

Sicherheitsfrage*

Abschicken

Zertifikat nicht gefunden? Hilfe und Kontakt

Bitte rechnen Sie 4 plus 2.

WIFI ZERTIFIZIERUNGSSTELLE

WIFI-ZERTIFIKATE SCHIEDSSTELLE INTRANET

Suchwort eingeben Finden

Startseite > Personenzertifikate > Zertifikatsdatenbank

Suche

Suche nach Personen Suche nach Zertifikaten

Zur Person und Nachnamen eingeben
Baumann

Baumann MSC.

Baumann

Zertifikat	Titel	Gültigkeitsbereich	Wissensbereich	Gültig bis
150102350	Immobilienmakler-Assistentin	IMMA1550002		12.12.2019

BAUMANN
Baumann
Baumann MSC.
BAUMANN
Mag. Baumann

Lösungsansatz - Ziele

- Ziele
 - Digitale Verwaltung und Dokumentation von
 - Zertifikatsdaten
 - incl. digitaler Signatur
 - Zertifizierungsstellen
 - ... weitere Stammdaten
 - Standardisierte Möglichkeit zur
 - Publikation
 - Suche/Beauskunftung
 - Überprüfung der Gültigkeit
 - Anbieter- (Zertifizierungsstellen-) übergreifend
- => massive Organisationsvereinfachung

Lösungsansatz – Blockchain

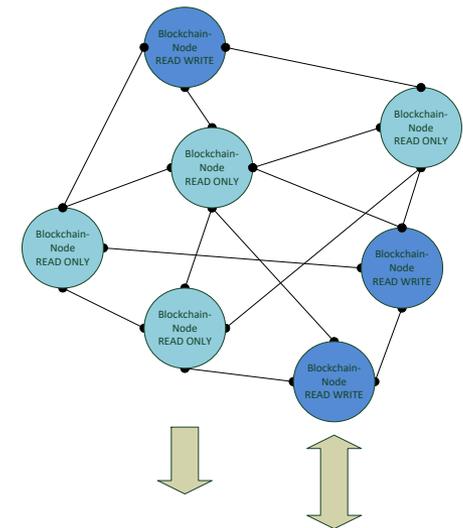
- Daten in „gemeinsamer“ (anbieterübergreifender) „Datenbank“ zusammenführen
 - Definierte Datenstruktur
- Services für Information/Beauskunftung
 - Jeder Anbieter (wie bisher, Branding)
 - Neutral (über gesamten Datenbestand)
- Zusatzservices
 - Automatisierte Validierung
 - Z.B. Schnittstellen für Fachanwendungen
 - Mobile Lösungen
 - Z.B. QR-Scan basierende Auskunft
 - ...

Warum Blockchain-Ansatz?

- Dezentral
 - Kein einzelner, spezieller „Systembetreiber“, „Datenowner“ ... (Gleichberechtigung)
 - Robust (ausfallssicher ggü. Zerstörung, Zensur)
- Transparent
 - Konsistente Sicht aller Beteiligten auf alle Daten
 - „eine Wahrheit“, lokale Datenverfälschung (Absicht, Systemfehler, Angriff ...) würde erkannt werden
- Unveränderbar
 - Bestehende Daten unveränderbar/unlöschar
 - Neue Daten nur hinzufügen

Details Systemteilnehmer

- Regel/Vereinbarung
 - „Jeder Teilnehmer betreibt einen Blockchain-Node“
 - Ibs. schreibende Teilnehmer
- Teilnehmer
 - Zertifizierungsstellen
 - Akkreditierungsstelle (BMDW)
 - Interessensvertretungen (WKO, AK ...)
 - Nutzer der Daten (Suche, Validierung)
 - Serviceprovider
 - Unternehmen (z.B. Generalunternehmer im Baubereich, ...)



Details Zugriffsrechte

- Schreiben
 - Zertifizierungsstellen (Zertifikate)
 - Akkreditierungsstelle (Zertifizierungsstellen)
- Lesen
 - alle

		Validierung (schreiben)	
		<i>Permissionless</i>	<i>Permissioned</i>
Zugriff (lesen)	<i>Public</i>	Kryptowährungen ... (öffentlich)	Register, Zertifikate ... (veröffentlichen)
	<i>Private</i>	(n/a)	Banken, Versicherungen ... (intern, „Konsortium“)

Details DSGVO 1

- Aktuelle Sichtweise Zertifizierungsstellen
 - „... Abfragemöglichkeit vorübergehend eingestellt ...“
 - „... Zertifikatsinhaber muss (Veröffentlichung) zustimmen ...“
 - Widerspruch zur Veröffentlichungspflicht?
 - => rechtliche Klärung – auch als Basis für ähnliche Fragestellungen

Details DSGVO 2

- Recht auf ... „Vergessenwerden“ (auch Korrektur)
 - „Blockchain vergisst nie“
- Widerspruch => Lösungsansatz
 - Personenbezogene Daten „offchain“ (z.B. dezentrales Filesystem)
 - Meta-Informationen incl. Bestätigung (PoE, Notarization) plus Link „onchain“
 - Wenn nötig, pb. Daten (physisch) löschen oder Verknüpfung löschen
 - Ev. Lösungsansatz über Identitymanagement?
 - „Recht auf eigene Identität ...“

Weitere Aspekte Blockchain-Ansatz

- Interoperabilität
 - Blockchain-Nodes als gemeinsamer Nenner
 - Automatische Synchronisation im verteilten Netzwerk
 - Automatische Erkennung neue Nodes
- Kosten
 - Opensource, alle OS-Plattformen
 - Libraries in allen gängigen Programmiersprachen
 - Zugriff von eigenem System über klar definierte APIs
 - Einfache Konfiguration (Firewall ...)

Prototyp/Beispiel: Abbildung von Zertifikaten in einer Blockchain

Stream: cert-test1 – 99 of 99 items

Publishers	AdminNode (1DDbVasYW8b1Vq5FM9ezpUnLcYGZ9pqE2XN6Cm)
Key	18B1029Z0027
Data	{"nn":"Z\u00f6chling","vn":"Georg","ti":"","tn":"MDes","pt":"Certified E-Commerce && Social Media Expert CESE ","zert_id":"18B1029Z0027","ablauf":"04.03.2021"}
Added	2018-04-11 06:32:46 GMT

Publishers	Seed node A3 (1GQrUoXuxwNuyKEgSmY7YJhZMX2gnLZXrTKYoQ)
Key	17D1001L0024
Data	{"nn":"Zocher","vn":"Daniel","ti":"Mag.,"tn":"","pt":"SCC - operativ t\u00e4tliche Mitarbeiter ","zert_id":"17D1001L0024","ablauf":"25.02.2028"}
Added	2018-04-11 06:32:46 GMT

Publishers	AdminNode (1DDbVasYW8b1Vq5FM9ezpUnLcYGZ9pqE2XN6Cm)
Key	18B1028D0016
Data	{"nn":"Zitt","vn":"Stefan","ti":"","tn":"BSc","pt":"Datenschutzbeauftragt[QBfKMU] ","zert_id":"18B1028D0016","ablauf":"27.02.2021"}
Added	2018-04-11 06:32:46 GMT

Nutzen 1

- Für Zertifizierungsstellen
 - Interoperabilität mit Gesamtsystem
 - Zusatzservices anbieten (Suche, Validierung, auch mit Daten anderer ZS ...)
 - Dieselbe Technologie auch intern (z.B. Datenaustausch mit Filialen ...)
- Für Unternehmen
 - Papierprozesse werden anbieterübergreifend digitalisierbar
 - Definierte Schnittstellen für Fachanwendungen
 - Markttransparenz

Nutzen 2

- Für öffentliche Hand (BMDW)
 - Einblick in alle Zertifikate der akkreditierten Zertifizierungsstellen
 - ohne technischen oder finanziellen Aufwand
 - „muss kein zentrales System entwerfen/bauen/fordern ...“
 - Vorzeigeprojekt an der Schnittstelle zwischen digitaler Verwaltung und Unternehmen
 - Pionier in Europa (Vorstellung während EU-Vorsitz)

Weitere potentielle Anwendungen

- Personen
 - Lizenzen/Berechtigungen: Führerscheine, Pilotenscheine
- Material
 - Eigenschaften auf Chargen bezogen
- Produkte
 - Produktzertifikate (Hersteller/Leistungserklärungen)
 - Ursprungszeugnisse (Produkt/Land)
- Verwendungsbescheinigungen
 - KFZ: § 57a StVO, Zulassungsscheine, Typenscheine
 - Aircraft: Airworthiness review certificate
- ... uvm

Zusammenfassung, Ausblick

- Blockchains in „Nicht-Kryptowährungs“-Bereichen
 - Supply-Chain, Transport/Logistik, Asset-Tracking, Notarization ...
 - „(öffentliche) Register“: Grundbuch ...
- Bereich Zertifikate
 - Sinnvoll, Nutzen ...
 - Hausaufgaben
 - Rechtlich, Technisch (DSGVO ...)
 - Als Proof of Concept bzw. Beispiel für
 - Ähnliche Anwendungsbereiche
 - EU-weite Systeme/Lösungen?

Kontakt

AUSTRIAPRO

<http://www.austriapro.at>
austriapro@wko.at

DI Dr. Christian Baumann
c.baumann@baumann.at
+43 664 43 24 243