



Identitäten für das digitale Gesundheitswesen Zertifikate und der Certificate Service Manager (CSM)

Datum: 11.11.2019

Agenda

Wozu digitale Zertifikate?

Der Weg zum Zertifikat - Certificate Service Manager (CSM)

Einsatzbeispiele für Zertifikate im Gesundheitswesen

Voraussetzungen für eHealth: Vertrauenswürdige Identitäten + Schutz von Patientendaten



Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus

1.4.2 Signatur von Nutzdatendateien

Die Signierung von Dateien dient der zusätzlichen Sicherung der Integrität und Authentizität der übertragenen Dateien. Dieses Verfahren wird bereits in den bisherigen Datenübermittlungsverfahren verwendet, war jedoch bislang nicht verpflichtend. Ab dem 1.10.2017 sind die zu übermittelnden Daten vom Absender zu signieren. Hierzu können die zur Verschlüsselung genutzten Zertifikate

7.13.8 Kryptographische Absicherung (dat)

Mit Hilfe eines Kryptographiekonzeptes können die Vertraulichkeit oder INTEGRITÄT von Informationen gewährleistet werden.

ANF-MN 113 Das Krankenhaus SOLL ein Kryptographiekonzept und ein kryptographisches Verfahren als auch das Schlüsselmanagement in den jeweiligen Anwendungsfelder (z.B. WLAN, VPN, SSID) festlegt. Das Konzept SOLL weiterhin festlegen, in welchen Anwendungsbereichen Verschlüsselung verbindlich einzusetzen ist.

22.10.2019

Datenübermittlung und Abrechnung von Krankenhausleistungen ab 1.1.2018

Umstellungshinweise für FTAM over IP

Zertifikate sind dabei die Personalausweise und TÜV-Plaketten der digitalen Welt



Personenzertifikate ermöglichen die sichere digitale Kommunikation und das elektronische Unterschreiben

- **Persönliche Zertifikate** werden für natürliche Personen ausgestellt, nachdem deren Identität geprüft wurde.
- Ein typischer Einsatzfall ist die **Signatur und Verschlüsselung von Email**, um die Identität der Kommunikationspartner zu verifizieren und Inhalte zu schützen.
- Bei der Digitalisierung papierbasierter Prozesse ermöglichen Signaturzertifikate **elektronische Unterschriften** von Dokumenten und die Freigabe von Prozessschritten.

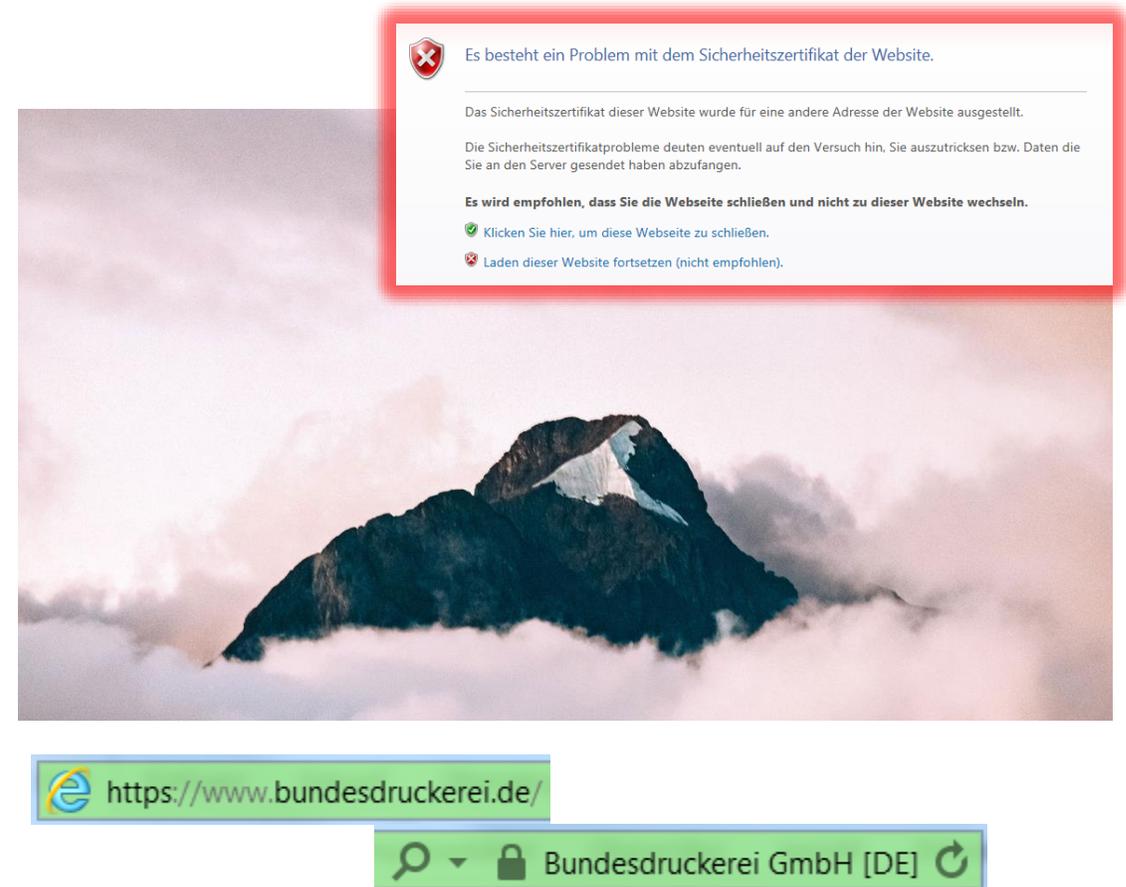


Server-Zertifikate schaffen Vertrauen in Web und Cloud und unterscheiden sich in der Validierung des Antragstellers

- **SSL-Zertifikate** werden für physische oder virtuelle Server ausgestellt, die öffentliche Dienste anbieten oder mit anderen Servern kommunizieren.

Beispiele für solche Dienste sind **Websites**, **Portale** für Patienten oder Mailserver.

- Die SSL-Zertifikate werden vom Server verwendet, um seine **Identität gegenüber dem Benutzer** nachzuweisen und um eine **verschlüsselte Kommunikation** aufzubauen.
- Abhängig vom Umfang der Prüfungen des Zertifikatsinhabers wird dem Benutzer visualisiert, ob die aufgerufene Website sicher ist.



Agenda

Wozu digitale Zertifikate?

Der Weg zum Zertifikat - Certificate Service Manager (CSM)

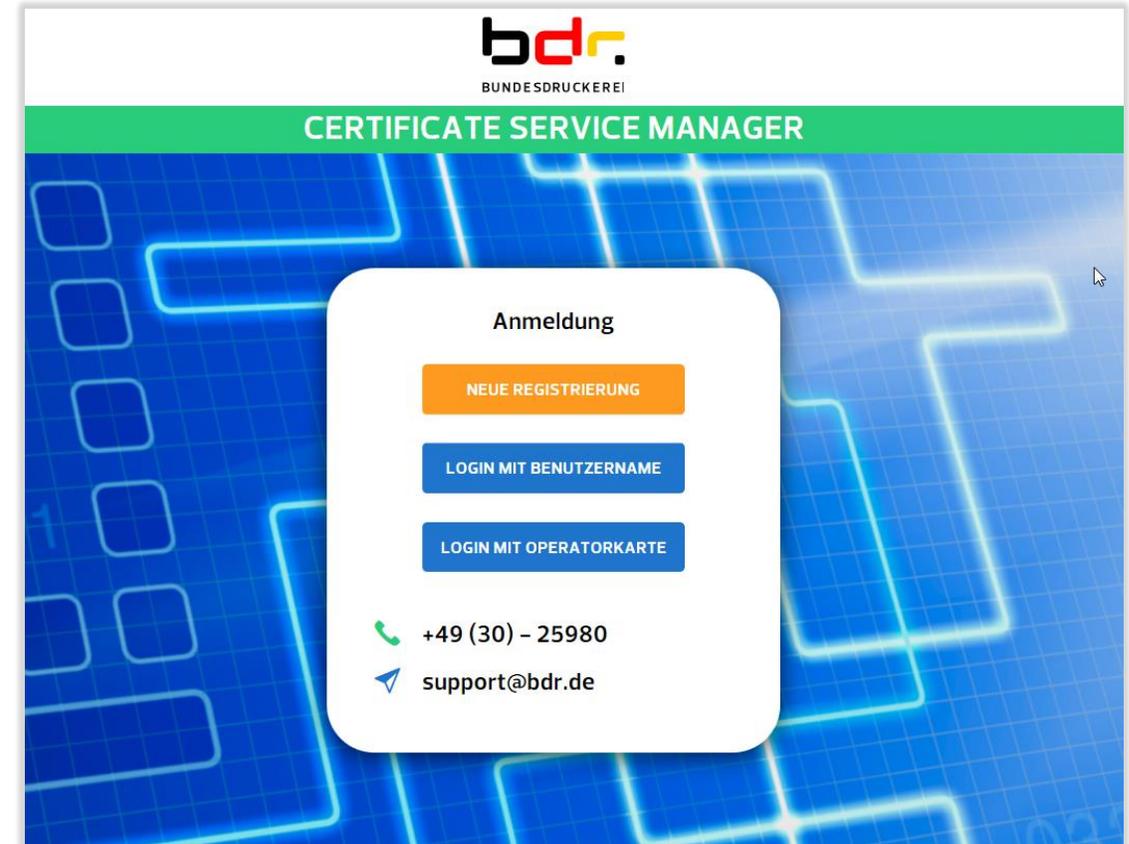
Einsatzbeispiele für Zertifikate im Gesundheitswesen

Klassische Beschaffungsprozesse für Zertifikate sind oft aufwändig und zeitraubend

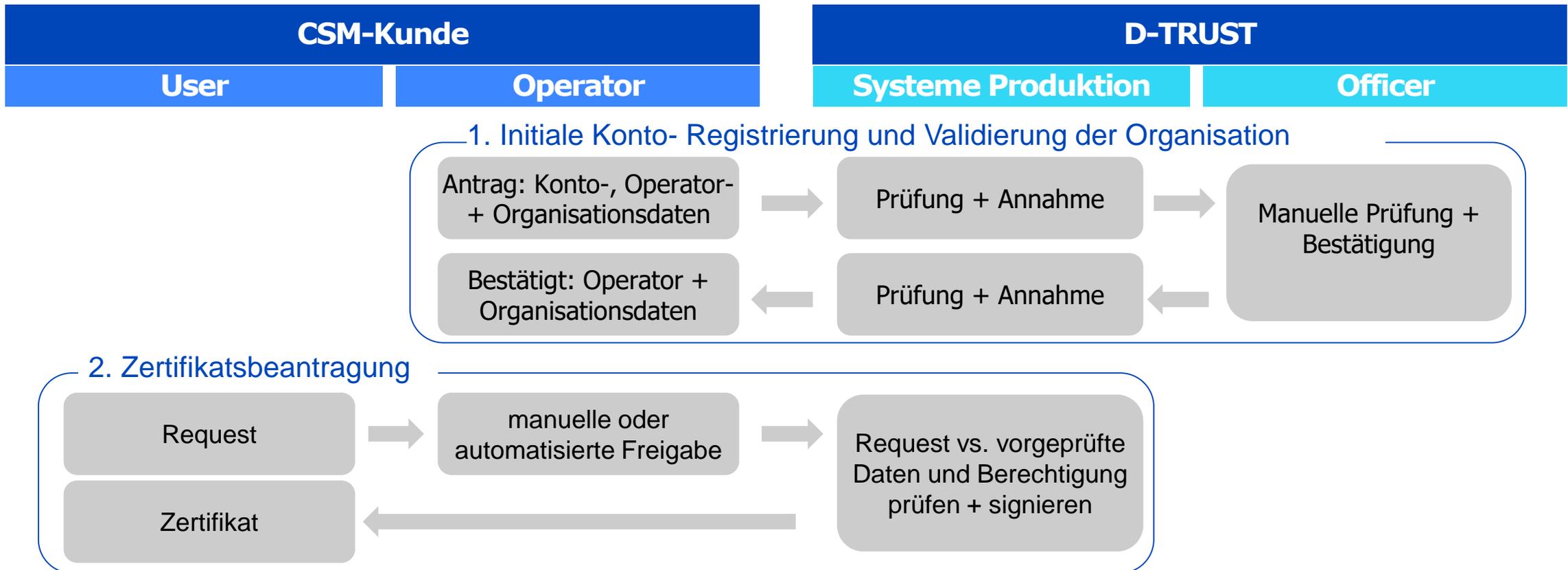
Schritt für Schritt zum Zertifikat	Zeitdauer ca.
Informationsphase	1 Woche
Angebotsanforderungsphase	1 Woche
Bestellphase 1 (kaufmännisch)	1 Woche
Bestellphase 2 (elektronisch) / Registrierung	15 Minuten
Validierung inklusive Rückfragen, Produktion	3 Werktage
Installation	15 Minuten

Der Certificate Service Manager (CSM) als Managed PKI bietet hier wichtige Vorteile

- **Vielzahl von Zertifikatstypen aus einer Hand**
 - für E-Mail, fortgeschrittene Signaturen und Siegel, SSL, Geräte, ...
- **Trennung** der Zertifikatsdatenprüfung von der Zertifikatsbeantragung + Erstellung
- dadurch **kurzfristige Ausstellung** von Zertifikaten manuell über Web-GUI oder über API
- **Identifikation** von Personen durch den Kunden
- zentralisierte **Verwaltung** des gesamten CSM-Zertifikatsbestands
- Online-Requestfreigabe durch **autorisierte Kunden-Operatoren**
- nutzungsabhängige Rechnungstellung



Nach einmaliger Registrierung und Validierung der Organisation werden Zertifikate direkt ausgestellt



Demo



CERTIFICATE SERVICE MANAGER (REF)

10203301

01011

Anmeldung

NEUE REGISTRIERUNG

LOGIN MIT BENUTZERNAME

LOGIN MIT OPERATORKARTE

+49 (30) - 25980

support@bdr.de

Agenda

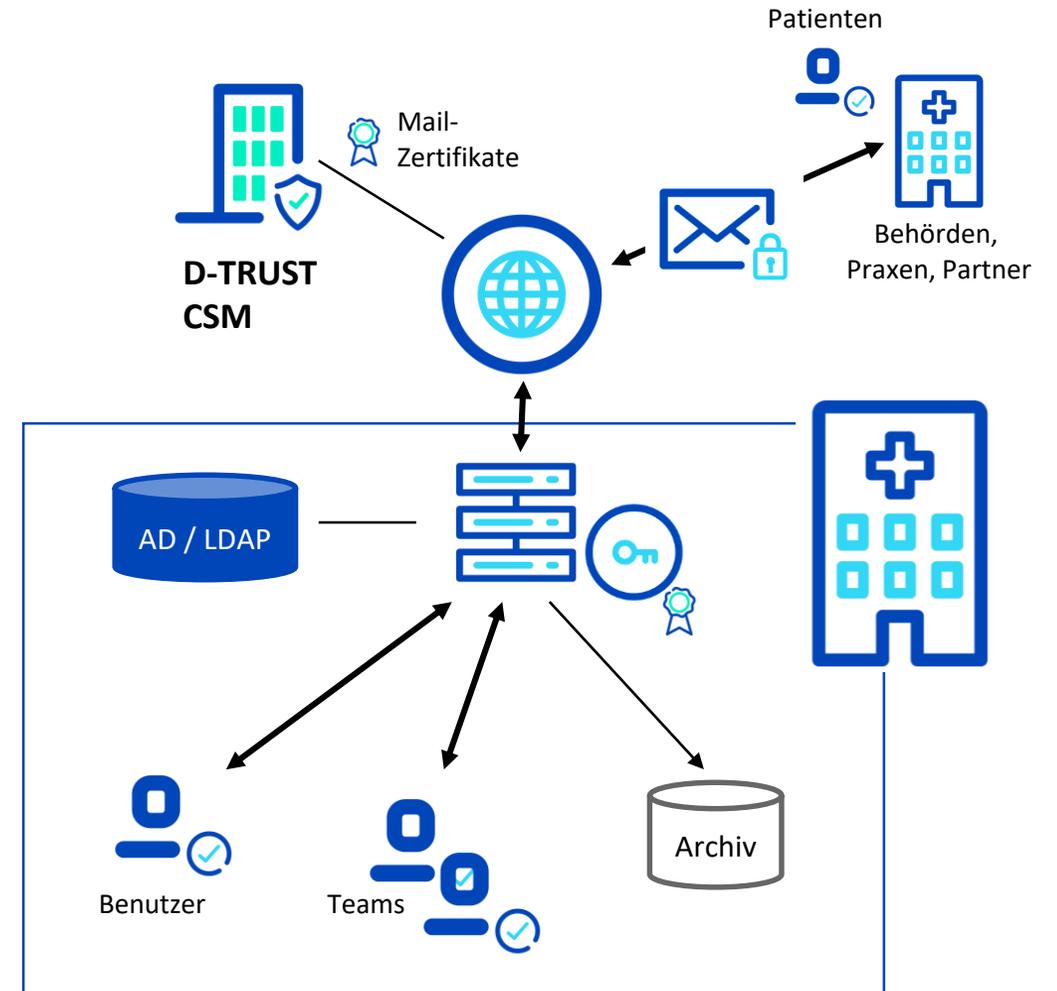
Wozu digitale Zertifikate?

Der Weg zum Zertifikat - Certificate Service Manager (CSM)

Einsatzbeispiele für Zertifikate im Gesundheitswesen

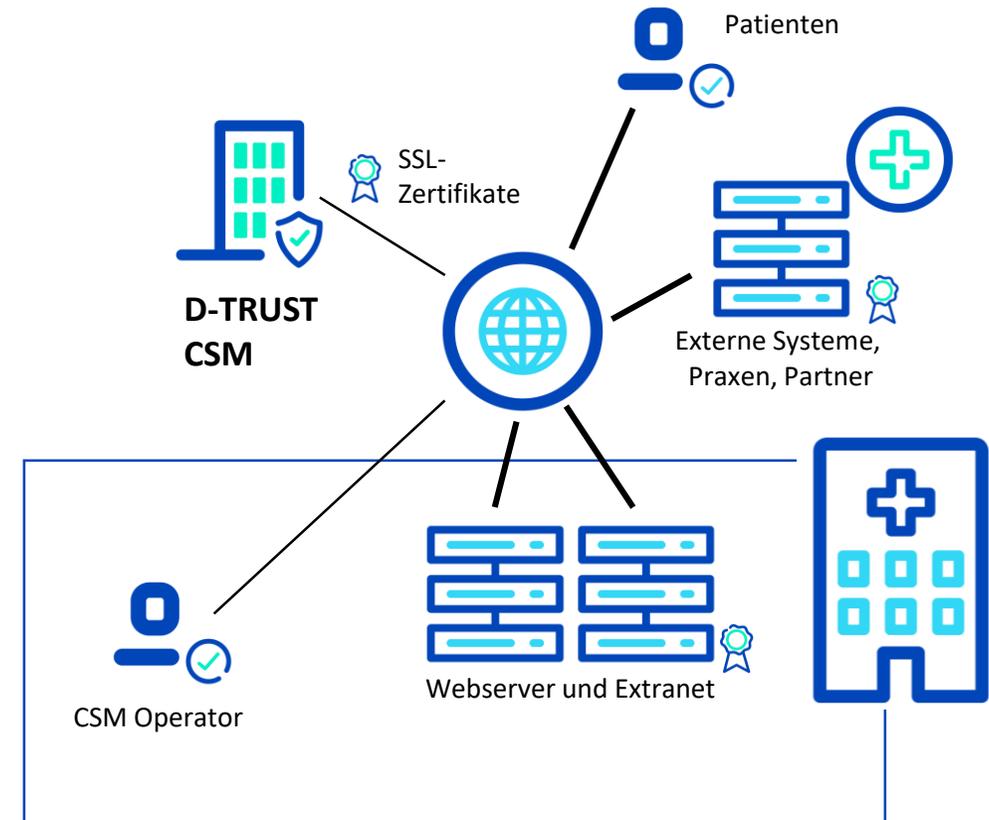
Signierte und verschlüsselte E-Mail mit Secure Mail Gateway

- Zertifikate für **Benutzer-** und **Team-Postfächer**
- **zentrales Mail-Gateway signiert** und **verschlüsselt** ausgehende E-Mails
- automatische Entschlüsselung und Signaturprüfung für eingehende Mails
- Gateway konfigurierbar über Policies
- **Malwareprüfung** und **Archivierung** am Gateway
- **automatischer Bezug und Erneuerung der Mail-Zertifikate** über CSM-Schnittstelle (API)
- Anbindung an Benutzerverzeichnis der Klinik (z.B. Active Directory) zur Berechtigungsprüfung
- **keine Installation** von Benutzerzertifikaten auf Clients oder Mobiles der Anwender erforderlich



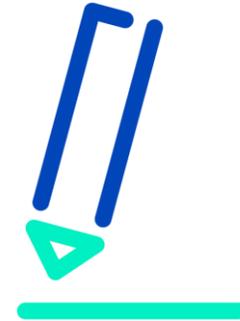
Sichere Kommunikation mit Servern und Webdiensten

- **SSL-Zertifikate** ermöglichen die **Authentisierung** von Servern und Webdiensten
- **verschlüsselte** Datenübertragung zwischen Servern und Clients
- Sicherer Webzugriff für Patienten auf **Patientenportale** über öffentliche Netze
- Zertifikate mit Organisationsattribut erhöhen dabei das Vertrauensniveau
- Remotezugang für **Mitarbeiter** auf Dienste wie Intranet und Webzugriff auf E-Mail
- Gesicherter Datenaustausch mit **externen Partnern**, z.B. für Radiologie
- Antragstellung für SSL-Zertifikate delegierbar, Freigabe durch den CSM-Operator der Klinik



Digitale Signatur und Siegeln von Urkunden + Bescheiden

- Digitales Unterschreiben von Dokumenten erlaubt **durchgängig digitale Prozesse**
 - **fortgeschrittene Signaturen** mit Zertifikaten aus dem CSM, z.B. für Freigaben in internen Workflows
 - **qualifizierte Signaturen** mit HBA oder Fernsignatur bei Schriftformerfordernis
- Digitale Siegel bestätigen die **Herkunft von Dokumenten** und deren Integrität
 - z.B. für ausgehende Schreiben als Teil eines automatisierten Workflows



Zertifikate sind ein wichtiger Baustein für digitale Identitäten und sichere Kommunikation im Gesundheitswesen

- **D-TRUST** als Trustcenter der Bundesdruckerei stellt als zertifizierter Trust Service Provider **öffentlich vertrauenswürdige Zertifikate** für viele Einsatzfälle bereit
 - sichere E-Mail
 - digitale Signaturen und Siegel
 - Absicherung von Servern und Webdiensten
- Der **Certificate Service Manager (CSM)** ist ein **komfortables Tool** für die Beschaffung und die Verwaltung dieser Zertifikate.



Ralf Dittmar

D-TRUST Consulting

E-Mail: ralf.dittmar@bdr.de

Telefon: +49 (0)30 25 98-2631

Vielen Dank. Und Ihre Fragen!

Hinweis: Diese Präsentation ist Eigentum der Bundesdruckerei GmbH.
Sämtliche Inhalte – auch auszugsweise – dürfen nicht ohne die Genehmigung der Bundesdruckerei GmbH vervielfältigt, weitergegeben oder veröffentlicht werden.

© 2019 by Bundesdruckerei GmbH.