Mit freundlicher Unterstützung:

bank-verlag

Informationstag
"Elektronische Signatur und Vertrauensdienste"
Gemeinsame Veranstaltung von TeleTrusT und VOI

Berlin, 18.09.2018

Starke Kunden Authentifizierung

Mark Rüdiger, procilon

procilon GROUP
Starke Kunden-Authentifizierung

18. September 2018

procilon Fakten

2001 gegründet
70 Mitarbeiter

Niederlassungen in Berlin & Dortmund

procilon SOFTWARE

Einzigartige Produktspektrum von Dateiverschlüsselung im Browser bis zu kompletten Infrastrukturen für Vertrauens-diensteanbieter nach eIDAS. Die Software-Entwicklung der procilon wurden nach Common Criteria EAL 4+ VAN5 (Angriffspotential hoch) auditiert und zertifiziert.

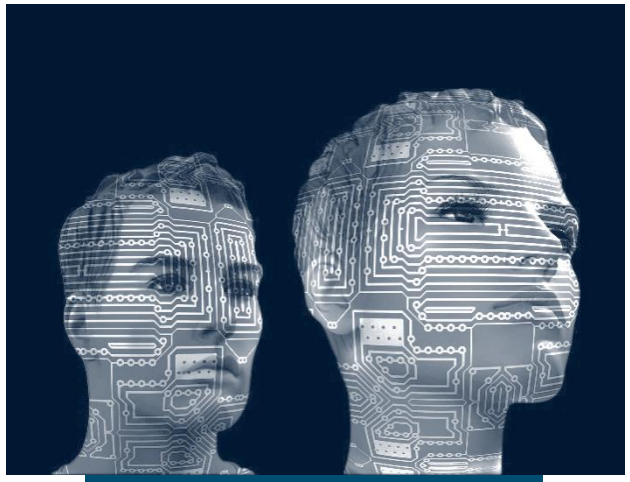
procilon BERATUNG

Die Beratungstätigkeit durch Datenschutz- und IT-Sicherheits-Spezialisten orientieren sich eng an nationalen und internationalen Standards und rechtlichen Vorgaben. Unter den Mitarbeitern finden sich zertifizierte ISO 27001 Auditoren genauso wie externe Datenschutzbeauftragte.

INFORMATIONSSICHERHEIT

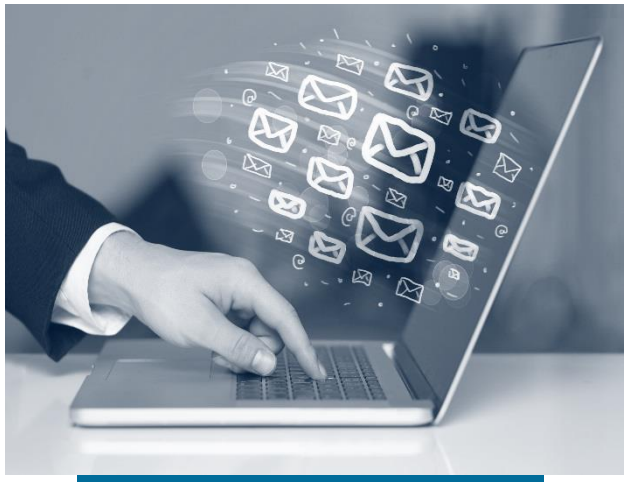
Geleitet vom Grundsatz Informationssicherheit als Ganzes zu betrachten, ist ein einzigartiges Lösungsangebot entstanden, das durch die Verbindung von Recht und Technik leistungsfähige Standardsoftware 'Made in Germany' genauso beinhaltet, wie die Planung und Umsetzung innovativer Individuallösungen.

KERNKOMPETENZEN & EIGENE LÖSUNGEN



IDENTITÄTEN

Erzeugung, Prüfung und Verwaltung elektronischer Identitäten auf jeweils notwendigem Sicherheitsniveau durch eigene PKI-Lösung



KOMMUNIKATION

Herstellung vertrauenswürdiger und vertraulicher elektronischer Kommunikation durch Signatur und Verschlüsselung

AUFBEWAHRUNG

Erfüllung der besonderen Anforderungen an nachweisbare und beweissichere elektronische Datenspeicherung

© Copyright by procilon | Technische Änderungen und Irrtümer vorbehalten

AUSGEWÄHLTE REFERENZEN

BUNDESNOTARKAMMER & DGN

NUTZEN

- moderne, zukunftsfähige **Trust Center-Infrastruktur**
- **Akkreditierung** als Vertrauensdiensteanbieter
- Erfüllung **höchster IT-Sicherheitsstandards**
- **Beweiswerterhaltung** im vollständig elektronischen Archiv

REFERENZ **Deutsches Gesundheitsnetz GmbH**

Modernisierung des Trust-Centers u. eIDAS-konformer Zeitstempeldienst

DGN Deutsches Gesundheitsnetz

Anwender
Deutsche Gesundheitsnetz

Branche
Gesundheitswesen

Herausforderung
- Modernisierung des seit 2007 durch BNetzA akkreditierten Trust Centers
- Einhaltung der durch eIDAS u. Vertrauensdienste-Gesetz geforderten Standards

Lösung
- Produktfamilie proNEXT
- Aufbau einer leistungsstarken, rechtskonformen Public Key Infrastructure
- Signaturanwendungskomponente auf Basis proNEXT Secure Framework

Besonderheiten
- qualifizierte Zertifikate/qualifizierter Zeitstempel-Service vor dem Hintergrund sich ändernder rechtlicher Rahmenbedin-

REFERENZ **Bundesnotarkammer**

Aufbau der Zertifizierungsstelle mit TrustCenter 1.0

BUNDESNOTARKAMMER
KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS

Anwender
Bundesnotarkammer

Branche
Öffentlicher Dienst

Herausforderung
- Entwicklung und Implementierung der technischen Komponente des Trust Centers der Bundesnotarkammer

Lösung
- PKI mit proNEXT Security Manager
- beweiswerterhaltende Langzeitarchivierung mit proNEXT Archive Manager
- EGVP-Integration mit proNEXT Communication Manager
- Signatur Anwendungs Komponente auf Basis proNEXT Secure Framework
- Beratung/Begleitung bei SigG-Bestätigung nach CC EAL4+VAN5

Besonderheiten

Zertifizierungsstelle der Bundesnotarkammer
Seit 2001 ist die Bundesnotarkammer (BNotK) von der Bundesnetzagentur (BNetzA) als Zertifizierungsdiensteanbieter (ZDA) akkreditiert. Die auf den qualifizierten Zertifikaten der Zertifizierungsstelle der Bundesnotarkammer beruhenden Signaturen genügen den umfassend geprüften technischen und administrativen Sicherheitsanforderungen nach § 15 Abs. 1 SigG. Damit erfüllen die von der Bundesnotarkammer ausgegebenen Signaturkarten die besonderen Anforderungen an die Erstellung notarieller elektronischer Urkunden. Sie kann von Notaren, Justizangehörigen und Rechtsanwälten beantragt werden. Ebenso gibt die Bundesnotarkammer qualifizierte Zeitstempel aus. Zur Zeit sind mehr als 17 250 ausgegebene Signaturkarten bei Notaren, Gerichten, Gerichtsvollziehern und Rechtsanwälten im Einsatz.

WILLKOMMEN

Signaturkarte beantragen »

beA-Karte beantragen »

Hinweise zu den neuen Signaturkarten

Alles Wichtige zur Signaturkarte

Austausch der Signaturkarten

© Copyright by procilon | Technische Änderungen und Irrtümer vorbehalten

PSD2 - Kontoschnittstelle – „OPEN BANKING“

- Banken **müssen** offen dokumentierte Schnittstelle bereitstellen, die es einem Third Party Provider (TPP) erlaubt, im Kundenauftrag auf Kundenkonten zuzugreifen
- betrifft ausschließlich online-fähige Zahlungskonten
- Bestätigung der Verfügbarkeit eines Geldbetrags (**Payment Instrument Issuer Payment Service Provider - PIISP** (Artikel 65))
- Zahlungsauslösedienste (**Payment Initiation Service - PIS** (Artikel 66))
- Kontoinformationsdienste (**Account Information Service - AIS** (Artikel 67))

- Was verändert sich also?
  - TPP erhalten in Echtzeit unmittelbaren Zugang zu sämtlichen Kontoinformationen des Kunden
  - Zahlungsanweisungen werden vom TPP elektronisch und im Namen des Kunden vorgelegt

© Copyright by procilon | Technische Änderungen und Irrtümer vorbehalten

Anforderungen PSD2 gemäß EBA-RTS

- **gesicherte Kommunikation** zwischen Bezahl-App und kontoführender Bank
- **Zwei-Faktor-Authentifizierung** (2FA) mit zwei Authentifizierungs-Elementen aus den Kategorien **Wissen**, **Besitz** und **Inhärenz**
- Dynamic Linking, Authentication-Code ist bei Fernzugriff **dynamisch** mit **Betrag** und **Empfänger** der Zahlung verknüpft
- Separated execution environment, auf Smartphone ist eine **sichere Ausführungs-umgebung** zu verwenden
- Zahlungsdienstleister muss sich für jeden Zugriff auf ein Konto identifizieren
  - Artikel 29 der RTS konkretisiert – Identifizierung mittels qualifizierter Zertifikate gemäß eIDAS (qualifizierte Webseiten-Zertifikate und Siegel)
  - Identifizierung des Zertifikatsinhabers durch VDA
  - die Sperrung von Zertifikaten
  - Erweiterung von Zertifikaten durch Angabe PSD2 spezifischer Attribute

© Copyright by procilon | Technische Änderungen und Irrtümer vorbehalten

CLOUD-SICHERHEIT

eIDAS

- einheitliche juristische Standards und IT Security Level
- geprüfte qualifizierte Vertrauensdiensteanbieter
- Interoperabilität und gegenseitige Anerkennung von elektronischen Identitäten in allen 27(+1) EU- und 4 EFTA-Mitgliedstaaten
- schafft Vertrauen in elektronischen Geschäftsprozessen
- Verbesserung der Akzeptanz durch Erleichterungen und Vereinfachung
- Liberalisierung im Binnenmarkt

© Copyright by procilon | Technische Änderungen und Irrtümer vorbehalten

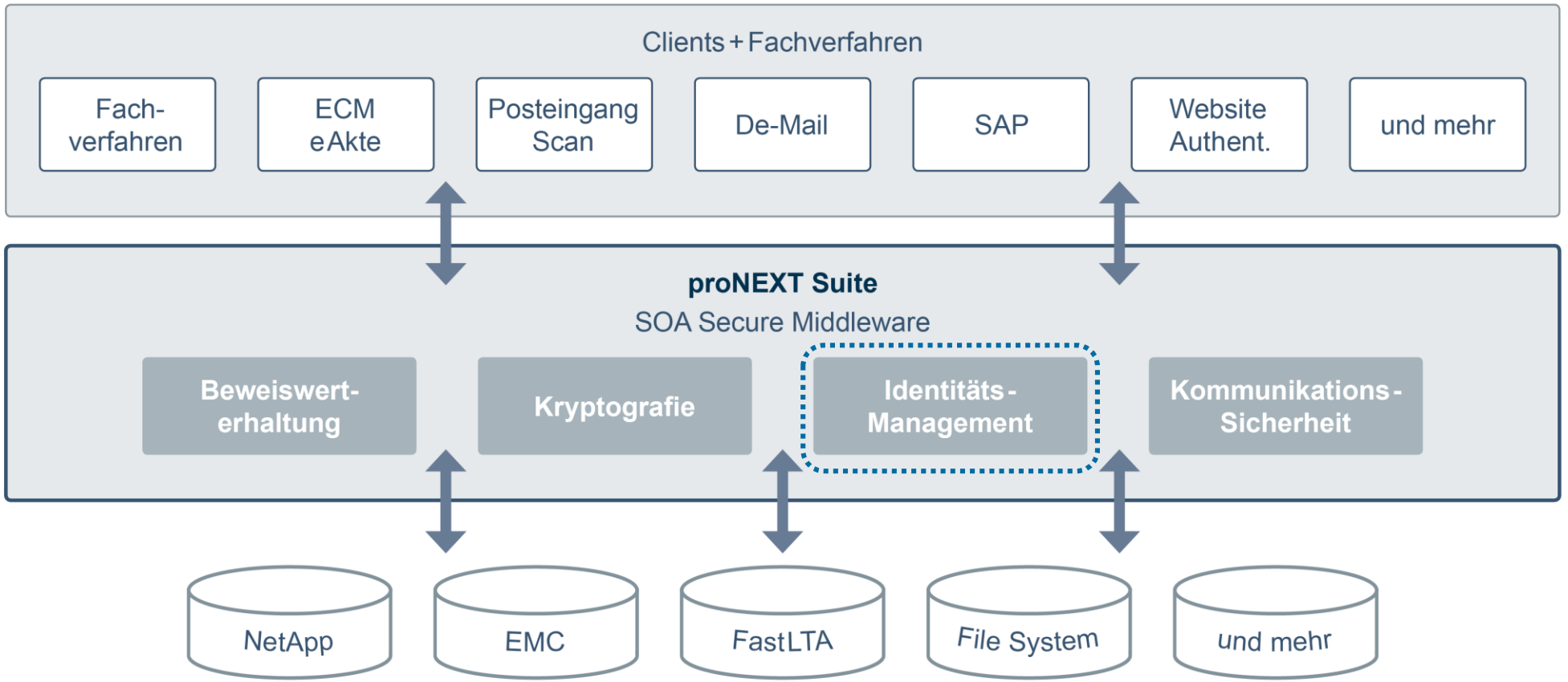
Zwei-Faktor-Auth. / dynamische Verknüpfung

- **Besitz:**
  - Bindung der Auth-App an das Smartphone durch Nutzung eindeutiger Gerätemerkmale - Smartphone des Benutzers kann als Besitzfaktor genutzt werden
- **Inhärenz** (Verknüpfung von Eigenschaften mit den Dingen, zu denen sie gehören):
  - Smartphones mit integrierten „Sensoren“ für Fingerabdrücke, Gesichtserkennung oder Iris-Scan
- **Wissen:**
  - Passwörter als klassischer Wissensfaktor zur Authentifizierung
  - Empfehlung der Vorgabe zur Verwendung starker Passwörter
- **dynamische Verknüpfung** unter Verwendung geheimer kryptografischer Schlüssel
  - z.B. durch Berechnung Authentication-Code über Empfänger & Betrag am Smartphone
  - **verschlüsselte Übertragung** zum Backend
  - **Vergleich** des empfangenen Authentication Code mit dem vom Backend berechneten Code

© Copyright by procilon | Technische Änderungen und Irrtümer vorbehalten

SCHEMATISCHE DARSTELLUNG

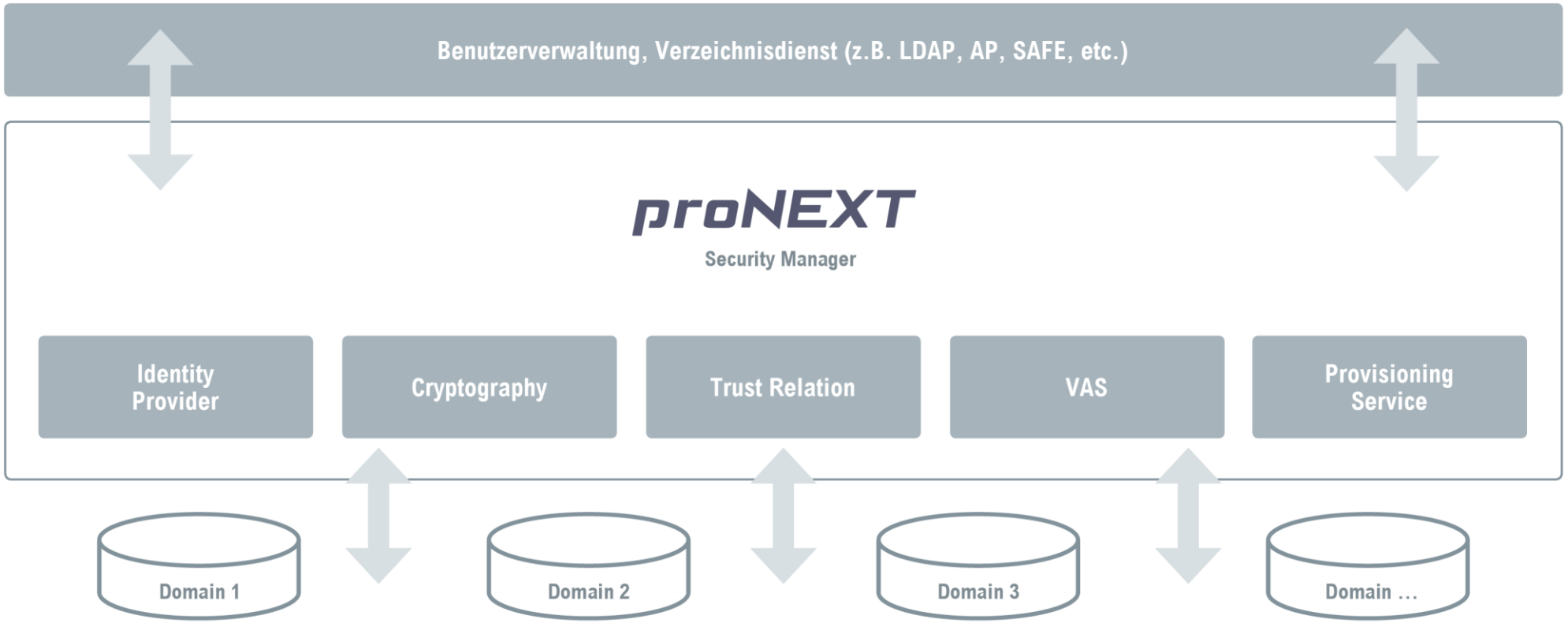
PRONEXT SUITE



© Copyright by procilon | Technische Änderungen und Irrtümer vorbehalten

SYSTEMARCHITEKTUR

PRONEXT SECURITY MANAGER (IAM)



VAS – virtueller Attributservice

© Copyright by procilon | Technische Änderungen und Irrtümer vorbehalten

VIELEN DANK

für Ihre Aufmerksamkeit

Mark Rüdiger

procilon GROUP
Leipziger Straße 110
04425 Taucha bei Leipzig

Telefon: 034298 4878-10
E-Mail: mark.ruediger@procilon.de

www.procilon.de