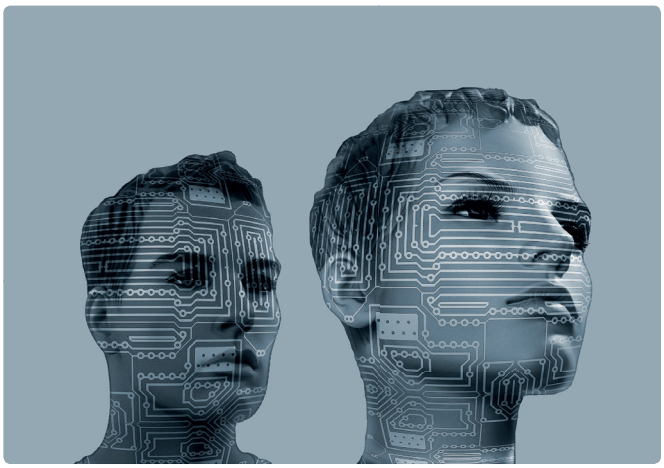
DATENBLATT **proNEXT Security Manager**

Sichere Authentifizierung und Identitätsverwaltung

- ✓ Umsetzung von Sicherheitsschutzzielen für elektronische Daten Identitäten
- ✓ konform zu Secure Access to Federated eJustice/E-Government (SAFE)
- ✓ realisiert starke Authentisierung gemäß PSD 2-Bankenschnittstelle
- ✓ eIDAS-konform
- ✓ Überprüfung nach CC EAL 4 + (Angriffspotential hoch) durch TÜV-IT

Die Herausforderung:

Der Alltag eines IT-Nutzers ist durch zahlreiche Anwendungen bestimmt, die sich gern auf abgeschlossenen Inseln befinden, unterschiedliche Sicherheits- und Authentifizierungs-Konzepte haben und den Menschen zu einem sorglosen Umgang mit seiner elektronischen Identität verleiten. Unterschiedlichste Authentisierungsmethoden beeinträchtigen zusätzlich die Akzeptanz.
Zur Klärung dieses komplexen Spannungsfeldes sind Lösungen erforderlich, die sich auf der einen Seite dynamisch an Nutzeraktivitäten anpassen und andererseits ein hohes Niveau von IT-Sicherheit erreichen. Mit einem Trusted-Domain-Konzept lassen sich diese Herausforderungen realistisch in der Praxis umsetzen.



Die Lösung:

Der proNEXT Security Manager bietet eine zentrale Identitätsverwaltung für alle Zugänge, beispielsweise zu Portalen, Fachanwendungen, E-Mail-Systemen, ERP-Software, Banksystemen sowie unternehmensweiten Ressourcen und Repositories. Die Verwaltung der zahlreichen, an die Anwender gebundenen Identifizierungs- und Authentifizierungsinstrumente wird damit leicht möglich. Durch das integrierte Berechtigungsmanagement erleichtert der proNEXT Security Manager die Zugangskontrolle. Der Anwender wird einmalig erfasst und registriert und ist dank einer Vertrauensstellung (im Sinne von Trusted Domains) für weitere bekannte Anwendungen zugriffsberechtigt. Eine erneute Autorisierung durch den jeweiligen Administrator entfällt, wodurch der Verwaltungsaufwand erheblich reduziert werden kann. Generell kann dies auch domainübergreifend erfolgen. Eine entsprechende Vereinbarung der jeweiligen Inhaber ist dann notwendig.

Exkurs SAML

SAML (Security Assertion Markup Language) ist ein XML-basiertes Framework, welches im Rahmen der Verwaltung elektronischer Identitäten und der Realisierung von Single-Sign-On-Szenarien eine wichtige Rolle einnimmt. Der SAML Standard unterteilt sich in verschiedene Bausteine. Den Kern bildet die Beschreibung von Identitätsinformationen durch eine festgelegte Struktur. Generell können komplexe Anwendungsszenarien realisiert werden (z.B.Web Browser Single-Sign-On).

Identitätsprovider

Der Identity Provider (IdP) verwaltet und steuert den sicheren Zugriff von internen und externen Anwendungen und ermöglicht die Abbildung von Vertrauensstellungen an zentraler Stelle. Er überprüft zusätzlich elektronische Ausweise (z.B. SAML-Token) auf ihre Gültigkeit und Berechtigung. Durch Authentifizierungs-Plugins, welche sehr einfach erweiterbar sind, sind neben herkömmlichen Anmeldeverfahren (Benutzername und Passwort) auch 2-Faktor-Authentifizierungen möglich. Diese Verfahren können auch in Kombination pro Anwendung festgelegt werden. Dadurch können Sicherheitsrichtlinien sehr einfach umgesetzt werden. Für die Nutzung verschiedener Anwendungen sind auch ein

DATENBLATT **proNEXT Security Manager**

Sichere Authentifizierung und Identitätsverwaltung

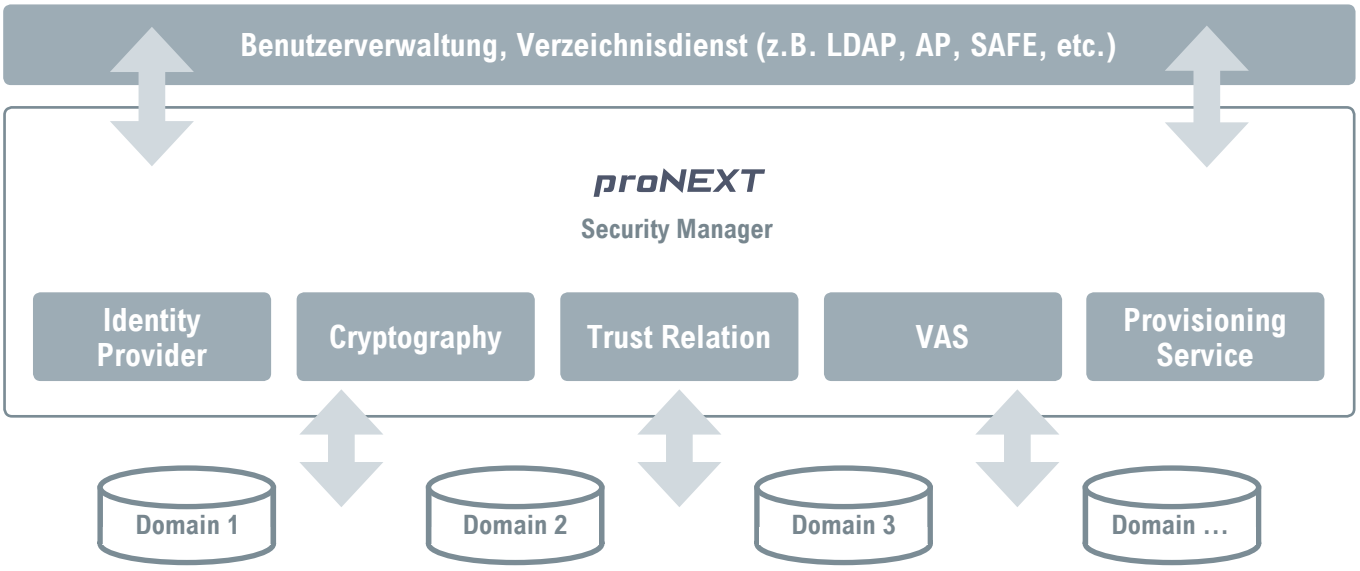
Single-Sign-On und dementsprechende Log-Out Funktionen implementiert. Über Filtermechanismen ist es möglich, verschiedenen Anwendungen bzw. Anwendungsteilen nur bestimmte Attribute zuzuordnen. Die jeweilige Autorisierungsentscheidung übernimmt die jeweilige Fachanwendung.

Attributsspeicher

Ein weiterer wichtiger Bestandteil ist der Attributsspeicher, welcher in Form eines LDAP genutzt wird. Die wichtigsten Attribute sind in diesem Attributsspeicher modelliert und werden in einem sehr flexiblen Schema vorgehalten.

Kryptografieservices

Weitere zentral zur Verfügung gestellte Dienste sind Funktionen zur serverseitigen Erstellung und Prüfung von digitalen Signaturen, der Ver- und Entschlüsselung. Diese können als Querschnittsdienste zum Integritätsschutz und zur Wahrung der Vertraulichkeit eingesetzt werden. Weiterhin wird damit einer unbemerkten Manipulation von Daten entgegengewirkt.
Ebenfalls integriert ist ein sicheres Self-Audit der Lösung, welches Bestandteil einer Evaluierung nach CC EAL 4+ (Angriffspotential hoch) war und die Integrität des proNEXT Security Managers selbst schützt.



Dieses kann bei Bedarf jederzeit erweitert und den fachlichen Bedürfnissen angepasst werden. Der Attributspeicher kann über den dazugehörigen Service und unter Berücksichtigung der jeweiligen Rechte des Anfragenden, Attribute lesend zugreifbar machen.

Vertrauensstellung

Neben den technischen Aspekten sind formale Vereinbarungen zu treffen. Dies ist insbesondere bei Vertrauensstellungen zwischen domainüberschreitenden Applikationen oder Services elementar. Technisch werden z. B. Informationen zu Token-Arten, Herausgebern oder Signaturen überprüft.

Provisionierungsservice

Ein Provisionierungsservice erlaubt die Anlage, das Modifizieren und Löschen von Identitäten. Weiterhin verbindet er Rollen und Rechte mit diesen Identitäten und berechtigt sie für entsprechende Anwendungen. Die Schnittstelle zur PKI ermöglicht einfaches Hinzufügen und Verwalten von Authentifizierungsmitteln.

Integrationsservice

Für Integrationsszenarien bietet die Lösung sichere Rest- bzw. Webservices nach internationalen Standards und berücksichtigt die aktuellen Kryptographie-Empfehlungen des BSI.

Kontakt

procilon GROUP
Leipziger Straße 110
04425 Taucha

+49 342 98 48 78-31
anfrage@procilon.de
www.procilon.de