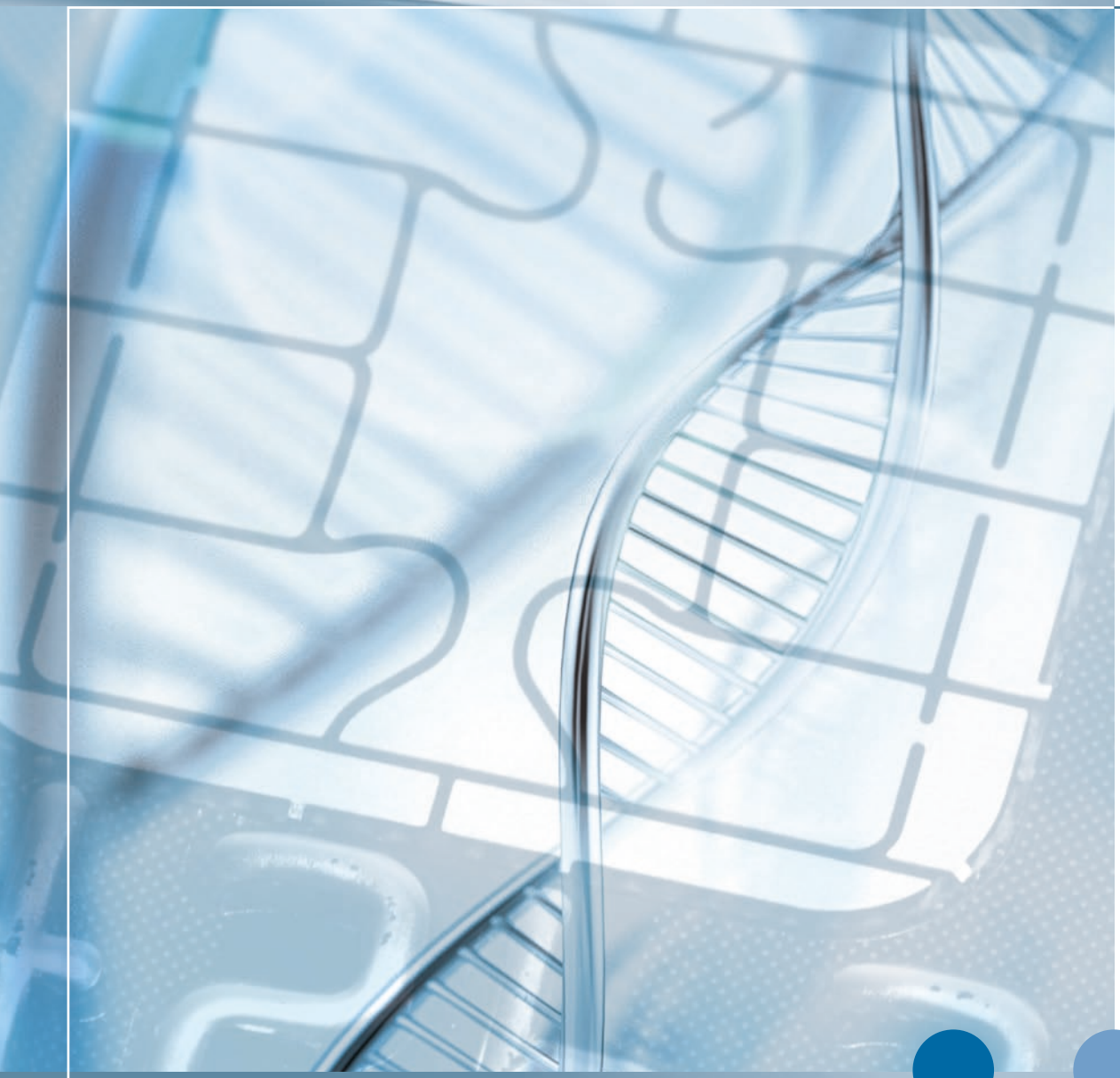
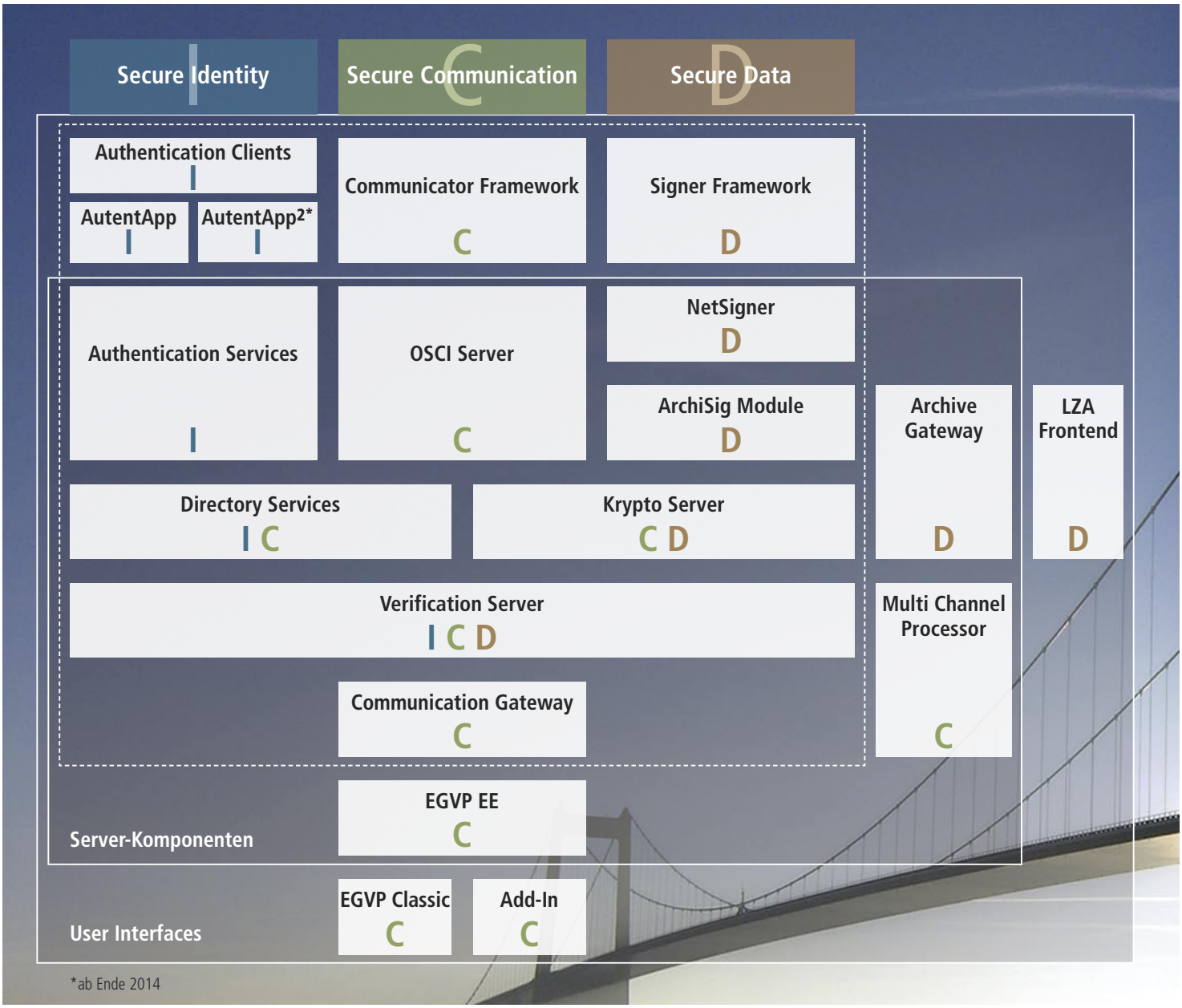
Governikus KG



Secure Identity Suite

Inhalt:

Komponentenübersicht



Secure Identity Suite

Im Zeitalter des World Wide Web werden Verwaltungs- und Geschäftsvorfälle sowie sonstige Transaktionen mehr und mehr elektronisch bzw. online abgewickelt. Die Vorteile liegen auf der Hand: Schnell, einfach und unkompliziert sorgen medienbruchfreie Prozesse und Dienstleistungen für Bürokratieabbau, Effizienzsteigerung, Kostenoptimierung und Fehlerquellenvermeidung.

In Punkto Identitätsnachweis sind die meisten Transaktionen jedoch nur bedingt vertrauenswürdig. In der Konsequenz werden Prozesse unter Umständen durch zusätzliche Sicherheitsmechanismen, wie z. B. ein postalisches Identverfahren, zu nicht mehr ganz medienbruchfreien Abläufen.

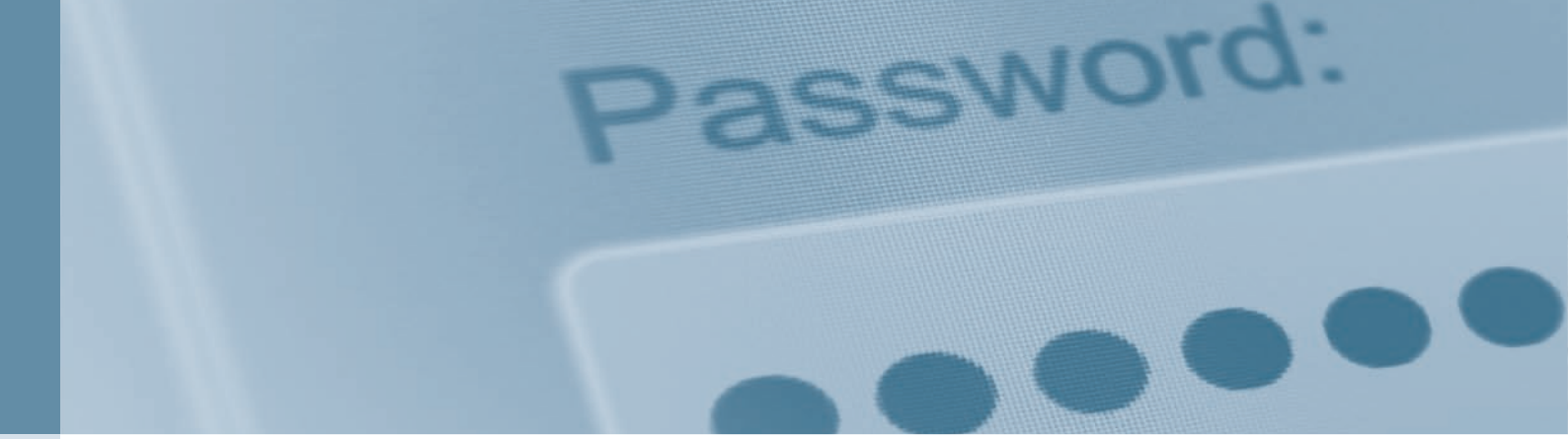
Vor allem die Einbindung zur Nutzung der eID-Funktion des Personalausweises und Aufenthaltstitels in vorhandene Infrastrukturen ermöglicht einen gegenseitigen Identitätsnachweis und sorgt für sichere und vertrauenswürdige Online-Transaktionen. BürgerInnen weisen sich mit Hilfe der eID-Funktion aus, der Diensteanbieter – ob nun Verwaltung, Online-Shop etc. – versichert anhand eines vom Bundesverwaltungsamt (BVA) autorisierten Berechtigungszertifikats seine Identität. Dabei sind Personalausweis und Aufenthaltstitel hoheitlich verbürgte Dokumente und werden zukünftig flächendeckend verbreitet sein.

Governikus steht für Sicherheit!

Governikus Lösungssuiten haben vor allem eines gemeinsam: Sie stehen für Sicherheit! Sicherheit in Bezug auf Rechtsverbindlichkeit, Sicherheit in Bezug auf Vertraulichkeit, Sicherheit in Bezug auf Gesetzeskonformität. Seit Gründung der Governikus KG im Jahr 1999 (damals unter dem Namen bremen online services) beschäftigen unsere Spezialisten sich intensiv mit dem Schutz personenbezogener Daten sowie nationalen und internationalen Gesetzeslagen. Dieses Know-how ist die Grundlage für unsere Entwicklungen.

Secure Identity: Elektronischer Identitätsnachweis!

Die Secure Identity Suite beinhaltet sämtliche Komponenten, die für unterschiedliche Einsatzszenarien rund um sichere Identitäten im Internet benötigt werden – sowohl Serverkomponenten als auch unterschiedliche User Interfaces.



Komponente Authentication Services

Die Komponente Authentication Services umfasst sowohl einen eID-Server als auch die Möglichkeit zur Umsetzung eines ganzheitlichen Konzeptes zur einfachen und kostengünstigen Integration von eID in vorhandene Infrastrukturen.

eID-Server Autent

Der Autent-Server ermöglicht – je nach sicherheitskritischem Einsatzszenario – neben der eID-Funktion des Personalausweises (PA) und Aufenthaltstitels (AT) auch eine Zertifikats- oder User- und Password-basierte Authentisierung. Dabei implementiert der Autent-Server das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlene eCard-API-Framework, welches plattformunabhängige Schnittstellen umfasst und die Kommunikation zwischen Anwendungen und Chipkarten vereinheitlicht. Gewährleistet wird über diese eCard-API neben der Anbindung an die Governikus Autent User Interfaces auch die Interoperabilität des Autent-Servers zur AusweisApp sowie sonstigen eID-Applets und Clientanwendungen.

Die wichtigsten Merkmale des Autent-Servers:

- Modularität
- Mandantenfähigkeit
- Integrationsschnittstellen für Fachanwendungen
- Interoperabilität durch eCard-API
- Implementiert unterschiedliche Berechtigungszertifikate
- Verwaltung des Berechtigungszertifikats
- Sperrlistenmanagement

Die Modularität des Autent-Servers gewährleistet darüber hinaus flexible Kombinationen aus den folgenden ID-Schnittstellen und Authentisierungsmethoden:

- Authentisierung mit PA und AT
- Zertifikatsbasierte Authentisierung
- Authentisierung mit Benutzernamen und Passwort
- ID-Schnittstelle nach TR-03130
- ID-Schnittstelle nach WebSSO Profile aus SAML 2.0
- STS nach WS-Trust

Bürgerkonto

Beim Bürgerkonto handelt es sich um ein ganzheitliches Konzept, basierend auf dem VITAKO-Prinzip, das Kommunen die kostengünstige und einfache Integration der eID-Funktion in ihre Online-Services ermöglicht. Das Konto bündelt die direkte Kommunikation mit dem Autent-Server und stellt den Fachverfahren eine vereinfachte Schnittstelle auf Basis des http-/https-Protokolls zur Verfügung.

Von der einfachen Anbindung abgesehen, hat das Konzept des Bürgerkontos einen weiteren Vorteil: Die Beantragung unterschiedlicher, verfahrensspezifischer Berechtigungszertifikate entfällt – es wird lediglich EIN Berechtigungszertifikat benötigt.

Sicher und innovativ:
eID-Server und User Interfaces
zur Authentisierung

Komponente AutentApp

Bei der Governikus Komponente AutentApp handelt es sich um ein Java-basiertes Applet mit lediglich 2 MB Speicherplatzbedarf, das wie auch der Autent-Server das eCard-API-Framework implementiert. Mit der AutentApp steht somit ein User Interface zur Verfügung, das sich einerseits problemlos in vorhandene Anwendungen integrieren lässt, andererseits folgende wichtige Merkmale bereitstellt:

- Anzeige von Berechtigungszertifikaten
- Auswahl von Merkmalskategorien
- Schnittstellen zu Identity Protocols

Die AutentApp interagiert mit dem Autent-Server, eine Anbindung an andere eID-Server ist mit der Komponente AutentApp² vorgesehen.

Komponente AutentApp²

Die Governikus AutentApp² (voraussichtlich verfügbar ab Ende 2014) wird mit einem einheitlichen eID-Kernel auf Basis von C++ plattformübergreifend als nutzerfreundliche und schlanke Anwendung für die Verwendung der eID-Funktion des Personalausweises und Aufenthaltstitel zur Verfügung stehen. Die AutentApp² kann auch außerhalb und unabhängig von den Governikus Lösungssuiten von allen BürgerInnen eingesetzt werden, sprich sie interagiert auch mit anderen am Markt verfügbaren eID-Servern.

Unterstützt werden dabei zunächst die Betriebssysteme ab Windows 7, Windows 8.1 sowie MacOS 10.9 im stationären Umfeld sowie Android ab 4.3 und iOS 7.

Komponente Authentication Clients

Für die zertifikatsbasierte Authentisierung in Verbindung mit dem Autent-Server stehen weitere User Interfaces zur Verfügung.

Komponente Directory Services

Das zentrale Modul für die Verwaltung von und den Zugriff auf digitale Identitäten ist die Komponente Directory Services. Mit dem Blick auf S.A.F.E.-Konformität auf der einen und Offenheit auf der anderen Seite bündelt diese Komponente alle Funktionalitäten, die eine moderne webbasierte Identity-Management-Lösung benötigt. In Verbindung mit dem Autent-Server lässt sich auf diese Weise ein S.A.F.E.-konformer Registrierungsserver realisieren.

Der Zugriff auf diese Komponente erfolgt authentisiert, ein umfangreiches Rollenkonzept schützt die hinterlegten Daten vor unberechtigter Einsicht und Manipulation. Die sichere Nutzung der Schnittstellen zur Verzeichnisabfrage und zur Registrierung ist über standardisierte WebService-Schnittstellen und über eine HTML-basierte Webanwendung möglich.

Die Directory Services verfügen über eine integrierte Benutzerverwaltung, die eine digitale Entität des Benutzers mit einer nahezu unbeschränkten Menge an zusätzlichen Attributen verknüpfen kann. Darüber hinaus lassen sich andere Verzeichnisdienste, wie Active Directory oder LDAP, integrieren. Fachanwendungen können spezifische Attribute hinterlegen, die mandantenspezifisch abgefragt und verwendet werden können. Als Hintergrunddienst stellen die Directory Services Nutzerinformationen für die Authentisierungs- und Kommunikationskomponenten zur Verfügung.

Komponente Verification Server

Der Governikus Verification Server stellt für alle Governikus Suiten (Secure Data, Secure Communication und Secure Identity) für vor- und nachgelagerte Komponenten die zentralen Funktionen zur Prüfung von Zertifikaten bereit.

Dieses sind die

- Bildung des Vertrauenspfads (vom Nutzer- bis zum Wurzelzertifikat),
- Prüfung der Signaturen der Zertifikate der Kette bis zum Wurzelzertifikat,
- Ermittlung des Sperrstatus der Zertifikate beim ausstellenden Trustcenter (online),
- Prüfung, ob der Signierzeitpunkt innerhalb des Gültigkeitsintervalls des Zertifikats liegt.

Geprüft werden können in der Standardkonfiguration des Verification Servers

- Qualifizierte Zertifikate, ausgestellt von deutschen Trustcentern (ZDA),
- Fortgeschrittene Zertifikate aus den Landes-PKIs (unter der PKI-1-Verwaltung) und
- Authentisierungs- und/oder Verschlüsselungszertifikate, soweit sich diese auf qualifizierten Signaturkarten befinden.

Die Konfiguration kann individuell erweitert werden.

Der Verification Server ist eine Signaturanwendungskomponente im Sinne des deutschen Signaturgesetzes. Die Prüfung qualifizierter Zertifikate, herausgegeben von deutschen ZDA, erfüllt vollständig die Anforderungen des deutschen Signaturgesetzes und der deutschen Signaturverordnung.

Internationale Zertifikatsprüfung und Trustcenter (ZDA)

Prüfbar sind alle X509 V3-Zertifikate unter Berücksichtigung der Profilierung gemäß CommonPKI. Europäische Signaturen sind über die im EU Large Scale Pilot PEPPOL profilierte XKMS-Responder entsprechend eingebunden und weitestgehend prüfbar.

Plattformunabhängig

Der Systemaufbau des Governikus Verification Server orientiert sich am Paradigma von SOA und gewährleistet dadurch eine flexible Einbindung in unterschiedlichste Systemlandschaften und -szenarien über Web-Services. Sämtliche Komponenten von Governikus basieren auf der bewährten Java-Technologie, die eine weitestgehende Plattformunabhängigkeit gewährleistet.

Der Governikus Verification Server läuft auf einem JBoss-Anwendungsserver. Ein Load-Balancer-Betrieb ist möglich und im Einsatz.

Produkt Governikus® Autent

Authentisierung auf höchstem Niveau

Sowohl Autent-Server als auch die AutentApp (sowie perspektivisch die AutentApp²) bzw. Authentication Clients stehen zusammengefasst als das Produkt Governikus Autent zur Verfügung.

Unsere Lösung wurde unter Berücksichtigung sämtlicher relevanten Technischen Richtlinien des BSI, internationalen Standards sowie rechtlichen Grundlagen entwickelt und ermöglicht medienbruchfreie Prozesse, die durch Einbindung der eID-Funktion des Personalausweises und Aufenthaltstitels dennoch sicher und vertrauenswürdig sind.

Best Practice-Ansatz gemäß „Brokered Authentication Pattern"

Zur Konzeption von Governikus Autent haben wir einen Best Practice-Ansatz gemäß Brokered Authentication Pattern gewählt. Zwischen einem Diensteanbieter und dem Autent-Server wird zunächst eine Vertrauensstellung erzeugt, indem die öffentlichen Schlüssel ausgetauscht werden. Der Diensteanbieter kann dann die Signatur des Autent Servers prüfen und somit sowohl die Integrität als auch die Authentizität der übermittelten Daten sicherstellen. Die zu übermittelnden Attribute für den Service Provider werden durch den Autent Server verschlüsselt.

Keep it small and simple

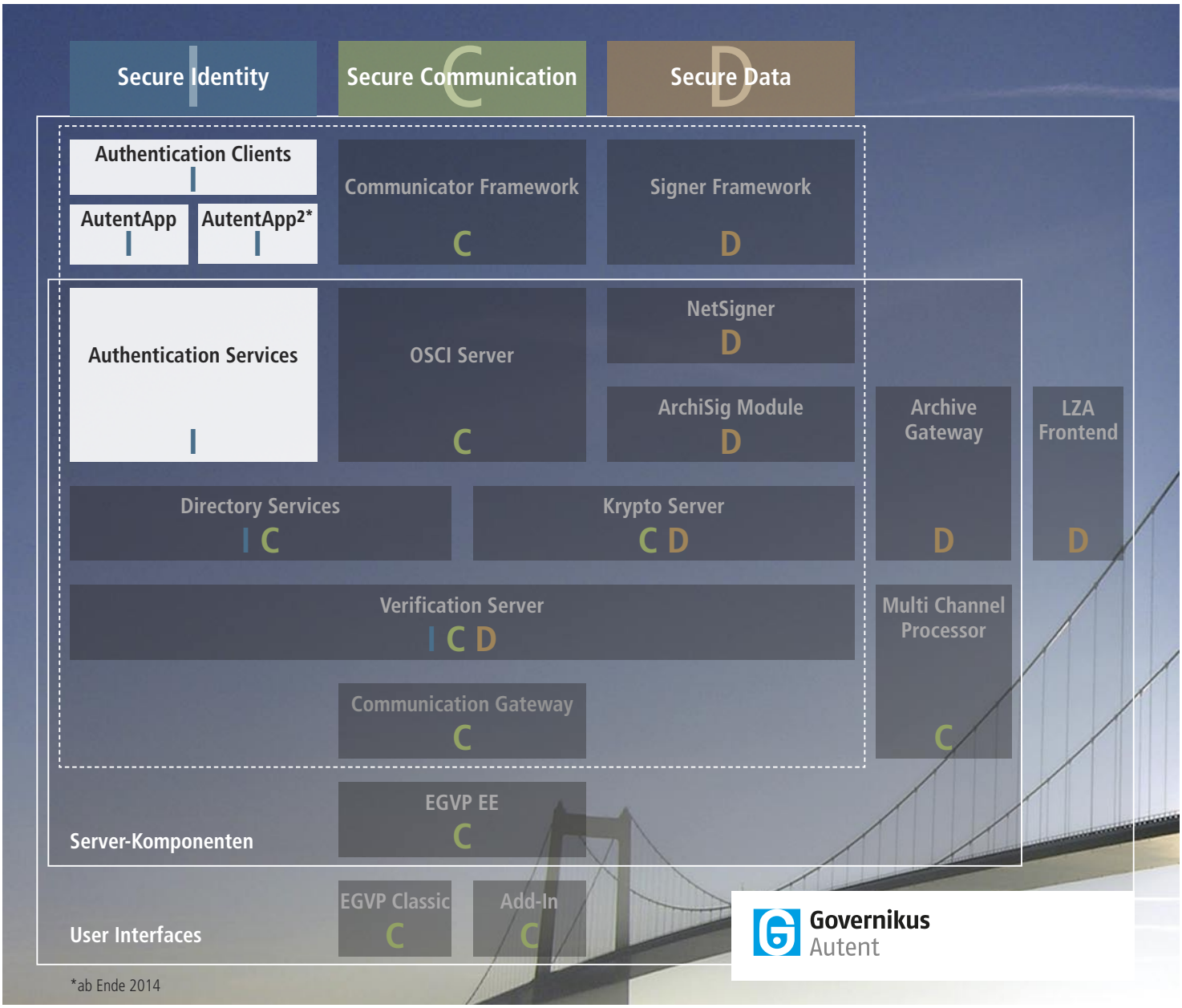
Vorteil für den Service Provider bei diesem Prinzip ist, dass er keine Verfahren zur Authentisierung bereitstellen muss. Ein weiterer Vorteil liegt in den flexiblen Authentisierungsverfahren. So ist z. B. die Verwendung einer Smartcard zur Anmeldung nicht für alle bereitgestellten Verfahren zwingend erforderlich. Weniger kritische Verfahren können beispielsweise auch User-/Password-basiert bereitgestellt werden.

Governikus® Autent als eID-Service

Einfach und kostentransparent stellen wir Governikus Autent auch als eID-Fullservice zur Verfügung. Unser Service wird in einem ISO 27001-zertifizierten Rechenzentrum betrieben, wir verfügen über das erforderliche Sicherheitskonzept und sind zertifiziert gemäß § 11 BDSG „Auftragsdatenverarbeitung".

Sicher und flexibel:
Vertrauenswürdige Online-Prozesse
durch Authentisierung

Komponentensicht Autent



Produkt Governikus® Bürgerkonto

Einfache eID-Integration – in Ihrer Portallösung oder im Governikus® Bürgerterminal

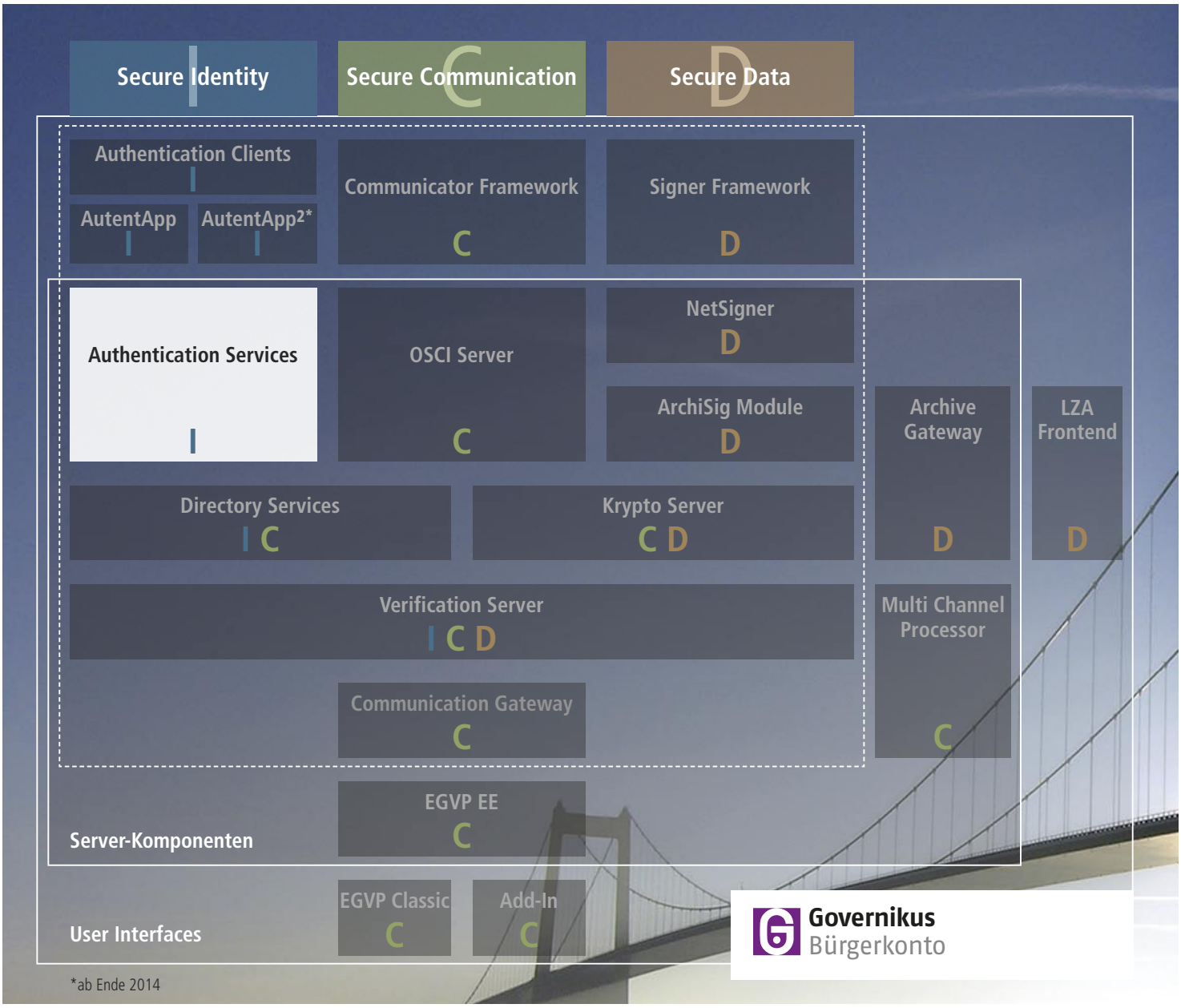
Das Governikus Bürgerkonto – Bestandteil der Komponente Authentication Services – ist ein temporäres Bürgerkonto nach dem VITAKO-Prinzip zur einfachen und kostengünstigen Integration unterschiedlicher Fachverfahren in Ihren Online-Portalen. Diverse Schnittstellen zu Fachverfahren wurden bereits realisiert, um einen weiteren Schritt auf dem Weg zur modernen Verwaltung zu machen.

Das Governikus Bürgerterminal ist ein Kooperationsprojekt von Governikus und führenden Herstellern kommunaler Fachsoftware – Telecomputer, Verlag für Standesamtswesen, HSH Soft- und Hardware Vertrieb, naviga und Kommunix. Am Governikus Bürgerterminal können sich BürgerInnen einfach und sicher mit der eID-Funktion von Personalausweis und Aufenthaltstitel ausweisen und so Verwaltungsdienstleistungen ohne Wartezeiten weitgehend selbstständig abwickeln. Dabei integriert das Governikus Bürgerterminal das Governikus Bürgerkonto.

Die Anbindung relevanter Online-Anwendungen aus Meldewesen, KFZ-Wesen, Gewerbewesen, Ausländerwesen und Personenstandswesen eröffnet Kommen, Städten und Landkreisen die Möglichkeit, ein breites Spektrum an Verwaltungsdienstleistungen mit dem PA/AT anzubieten.

Sicher und innovativ:
Best Practice-Ansatz zum Einsatz der
eID-Funktion von Personalausweis
und Aufenthaltstitel

Komponentensicht Bürgerkonto



Governikus KG

Governikus GmbH & Co. KG
Am Fallturm 9 | 28359 Bremen
Phone +49 421 204 95-0
Fax +49 421 204 95-11
E-Mail kontakt@governikus.com

Über uns

Seit 1999 beschäftigen wir uns mit den Themen Sicherheit und Vertraulichkeit in der elektronischen Kommunikation unter Berücksichtigung nationaler und internationaler Gesetzgebungen. Was mit dem mittlerweile in E-Government und E-Justice gesetzten OSCI-Standard und der ersten Transportanwendung Governikus begann, deckt heute den gesamten Zyklus elektronischer Kommunikation ab: von der Authentisierung über den sicheren Datentransport bis hin zur Beweissicherung und Beweiswerterhaltung elektronischer Daten. Gesetzeskonformität und somit Rechtssicherheit, Innovation sowie Interoperabilität und Investitionssicherheit stehen bei der Entwicklung unserer Lösungen im Vordergrund.

Authentisierung > Datentransport > Beweiswertige Daten

www.governikus.com

Stand: 3|2014