

03

ELAXY A²S

IT SOLUTIONS & SERVICES

> Sichere Authentifizierung und Autorisierung für Online-Banking und -Brokerage

Wie Sie die Sicherheit in Online-Banking und Online-Brokerage wirksam und kosteneffizient steigern, das Vertrauen Ihrer Kunden stärken und sich neue Umsatzpotenziale erschließen.

> VORTEILE AUF EINEN BLICK

- > Effektiver Schutz vor Angriffen sowie vor finanziellen und rechtlichen Schäden
- > Schnelle Integration und flexible Anpassung an individuelle Anforderungen
- > Höheres Kundenvertrauen verstärkt die Nutzung von Online-Banking und -Brokerage und senkt die Transaktionskosten
- > Flexible Skalierbarkeit z. B. für weitere eCommerce-Anwendungen oder Telefon-Banking über einen zentralen Authentifizierungsserver
- > Schnelle Reaktionen auf Missbrauchsversuche durch ständigen Überblick über Kundenzugriffe
- > Keine Abhängigkeit von proprietären Lösungen durch offene Standards
- > Minimaler Ressourcenaufwand ermöglicht volle Konzentration auf das Kerngeschäft

MEHR SICHERHEIT ALS WETTBEWERBSVORTEIL

Die wachsende Zahl krimineller Angriffe auf Banking- und Brokerage-Anwendungen durch Trojaner, Phishing oder Pharming verunsichern mehr und mehr Verbraucher. Ihre Kunden fragen sich zu Recht, wie sicher Banking im Internet wirklich ist und woran man geschützte Bank-Angebote erkennen kann.

Die Auswirkungen von Betrug und Datenklau durch mangelhafte Sicherheit sind nicht zu unterschätzen. Ein Imageverlust und fehlendes Vertrauen führen dazu, dass Kunden abwandern. Hier drohen empfindliche Umsatzeinbußen, bis zum Verlust der Wettbewerbsfähigkeit. Und auch juristische Konsequenzen sind möglich, wenn Sie die Einführung zwingend notwendiger Sicher-

heitsstandards vernachlässigen. Klar ist: Echte Sicherheit lässt sich nur durch wirksame Schutzmechanismen erreichen. Erst die Kombination aus Firewall, Virenschanner und Trojaner-Abwehr auf dem Kunden-PC plus dem von der Bank bereitgestellten Authentifizierungs- und Autorisierungssystem für Benutzer und Transaktionen erzeugt maximalen Schutz.

ELAXY A²S (ELAXY Authentifizierungs- und Autorisierungs-Server) bietet Ihnen leistungsstarke Funktionen zur sicheren Authentifizierung (z. B. Login) und Autorisierung (z. B. Passwort-Prüfung) für Ihre Online-Banking- und -Brokerage-Plattform – einfach integrierbar, kosteneffizient und mit maximalem Schutz vor Angriffen aus dem Internet. ■

DIE FAKTEN

1.000

A²S kann innerhalb kürzester Zeit bis **1.000TAN** Blöcke erstellen und verschlüsselt ablegen.

5

Für jeden Kunden können **gleichzeitig bis zu 5TAN** Blöcke angefordert werden.

SICHERE AUTHENTIFIZIERUNG UND AUTORISIERUNG

Das ELAXY A²S Modul ist die umfassende Lösung zur sicheren Authentifizierung und Autorisierung im Online-Banking. Dank offener Schnittstellen lassen sich vielfältige Web-Services und Fremdsysteme in bestehende System-Umgebungen und alle relevanten Applikationslandschaften integrieren.

Das ELAXY A²S Modul stellt folgende Ein- und Zweischrittverfahren bereit: **Passwort** (maximal fünf verschiedene Ausprägungen), **iTAN** (indizierte TAN) und **mTAN** (mobile TAN, SMS oder Handy-TAN). Durch den modularen Aufbau lässt sich A²S um weitere Sicherheits-

erweitern. Zusätzlich können Anwendungskomponenten wie die ELAXY e-Box integriert sowie Fremdsysteme wie SMS-Gateways und Druck-Provider angesteuert werden. Die schlanke Architektur ermöglicht minimale Zugriffszeiten von weit unter einer Sekunde, die eine optimale Nutzung innerhalb Ihrer Retail-Banking-

auch parallele Zugriffe durch andere Anwendungen kein Problem.

PASSWORT

Statische Passwörter, die sich selten ändern, bieten im Online-Banking weniger Sicherheit als dynamische Passwörter, deren Gültigkeit einen starken Zeit-Bezug haben (z. B. Einmal-Kennwörter).

Deshalb erzeugt A²S dynamische Passwörter mit folgenden Eigenschaften und Informationen:

- > Zuordnung Mandant zu Kundenkonto und Sicherheitsverfahren
- > Zeitpunkt der Erstellung und Ende der Gültigkeit
- > 5 verschiedene Passwort-Varianten (u. a. Super-PIN, PUC oder eigene Namen)
- > Generierungsart (systemgeneriert, benutzerdefiniert)
- > Verschlüsselungsverfahren für

„Maximale Sicherheit ist bei einem Authentifizierungs- und Autorisierungssystem das A und O. Bei der Evaluierung verschiedener Lösungen haben uns auch die einfache Integrierbarkeit und flexible Erweiterbarkeit von A²S überzeugt.

Thomas Blum, Implementation/Business Consulting der Fondsdepot Bank

und Verschlüsselungsverfahren wie Zertifikate und elektronische Signaturen Anwendung sicherstellen. Durch die Multi-Mandantenfähigkeit von A²S sind

> SICHERHEIT IM ONLINE BANKING

The screenshot shows the login interface of the Fondsdepot Bank. At the top left is the logo 'FONDSDEPOT BANK'. Below it is a blue header bar. The main content area is titled 'Legitimation' and contains the following text: 'Bitte legitimieren Sie sich mit Ihrer Zugangsnummer und Ihrer PIN:'. There are two input fields: 'Zugangsnummer:' and 'PIN:'. Below the input fields, there is a warning: 'Die Benutzung des Internets birgt Risiken. Bitte beachten Sie dazu auch unseren [Sicherheitshinweis](#). Mit der Eingabe der PIN akzeptiere ich die [Nutzungsbedingungen](#) für das Fondsbanking. Bevor Sie das Fondsbanking nutzen können, ist eine einmalige Freischaltung erforderlich. Das entsprechende Anmeldeformular erhalten Sie direkt bei Ihrem persönlichen Berater. Haben Sie ein **Allianz Global Investors Fondsdepot**? Dann steht Ihnen das Fondsportal unter www.allianzglobalinvestors.de zur Verfügung.' At the bottom of the form is a blue button labeled 'Anmelden'. At the very bottom of the page, there are links: '> Hilfe > Impressum > Konditionen > AGB'.

A²S im Einsatz: Der Anmeldevorgang (LOG-IN) für das Online Banking der Fondsdepot Bank aus Kundensicht. Um sich sicher im Kunden-Account einzuloggen, wird hier die Eingabe einer Zugangsnummer in Verbindung mit einer PIN benötigt. Durch die PIN-Eingabe wird die Identität des Kunden anhand der PIN Nummer überprüft (Authentifizierung).

Versand und interne Speicherung

- > Exportstatus und Zeitpunkt des Exports
- > Fehlbedienungs-zähler für jedes Sicherheitsverfahren

Jeder Aufruf eines Web-Service wird in A²S protokolliert und ist eindeutig nachvollziehbar. Zusätzliche Einstellungen können innerhalb von A²S für jedes der Passwörter vorgenommen werden. Ein Passwort kann für ein Kundenkonto nur dann erstellt werden, wenn ihm das entsprechende Verfahren zugeordnet und aktiviert ist.

iTAN

Während beim TAN-Verfahren der Kunde seinen Auftrag mit einer beliebigen TAN aus seiner Liste legitimiert, muss er beim iTAN-Verfahren in A²S eine durch Positionsnummer gekennzeichnete TAN aus einer durchnummerierten Liste eingeben. A²S erzeugt die entsprechenden TANS vorher im Modul und versendet diese verschlüsselt an den entsprechenden Druck-Provider. Dieser fasst die entschlüsselten iTANs in „Blöcken“ zusammen, druckt diese auf iTAN Bögen und liefert sie an den Endkunden aus.

Jede iTAN Aufforderung muss aus Sicherheitsgründen innerhalb weniger Sekunden durch Eingabe ausgeführt werden, da ansonsten ein Verbrauch in A²S erzeugt wird. A²S prüft jede Signatur einer iTAN durch Vergleich und gibt diese nur bei Übereinstimmung frei.

Folgende iTAN-Eigenschaften können in A²S festgelegt werden:

- > Anzahl iTANs
- > Zeichen und Länge der jew. iTAN
- > Zeitpunkt des Gültigkeitsendes von iTAN (in Sekunden) und iTAN-Block (in Monaten)
- > Verschlüsselungsverfahren für Ablage und Versand
- > Aktualisieren bei Falscheingabe durch Verlängerung der Eingabezeit

- oder autom. Verbrauch der iTAN
- > Anzahl der Falscheingaben von iTAN Nummern, danach Account Sperrung
- > Anzahl der Leer-Anforderungen des Index
- > Verfügungshinweis für iTAN: Wie viele Nummern stehen noch zur Verfügung?
- > Prozentsatz des iTAN Listenverbrauchs, bei dem die automatische Anforderung einer neuen iTAN-Liste erfolgt

Ein besonderes Sicherheitsplus ist dadurch gewährleistet, dass jede Session mit der jeweiligen TAN und dem Kundenkonto verknüpft ist. Bei Manipulationsversuchen lehnt A²S die Session ab, wenn beide Signaturen nicht identisch sind. Damit sind Manipulationen durch Trojaner nahezu ausgeschlossen.

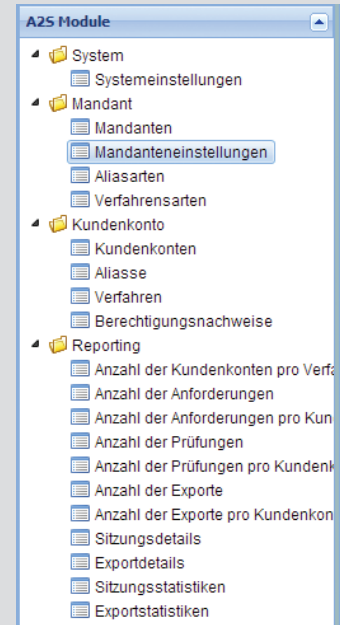
„A²S stärkt unsere Wettbewerbsfähigkeit nachhaltig. Es ließ sich schnell integrieren und die Betreuung von Seiten ELAXY ist jederzeit zuverlässig und professionell.“

Thomas Blum, Implementation/Business Consulting der Fondsdepot Bank

mTAN (SMS-TAN)

Bei einer mobilen TAN oder SMS-TAN wird dem Online-Banking-/Brokerage Kunden per SMS eine nur für diesen Vorgang verwendbare TAN auf sein Handy gesendet. Der Auftrag muss anschließend mit dieser TAN bestätigt werden. Durch den Medienbruch beim TAN-Ver-

> KOMFORTABLE ADMINISTRATION



Mit einem webbasierten Admin-Frontend bietet A²S die Möglichkeit, verschiedenste Einstellungen durchzuführen. Hier am Beispiel Mandanteneinstellungen.

sand bietet das mTAN-Verfahren mehr Sicherheit als das herkömmliche TAN- oder das iTAN-Verfahren. Der Signaturen-Vergleich beider SMS-TANs erhöht das Sicherheitsniveau zusätzlich.

A²S bietet flexible Einstellungsoptionen:

- > Zeichenart und -länge der SMS-TAN
- > Zeitraum der Nutzung (in Sekunden)
- > Anzahl der Falscheingaben
- > Versand einer Bestätigungs-SMS bei Freischaltung des Verfahrens

Wird das Gültigkeitsdatum überschritten, ist die TAN nicht mehr einsetzbar. Bei Falscheingabe kann die alte TAN gar nicht mehr oder maximal noch zwei Mal verwendet werden. ■

STARKE BASIS MIT FLEXIBLER SKALIERBARKEIT

Das ELAXY A²S Modul verfügt über einen umfassenden Funktionskern, der über ein Admin-Frontend und eine individuell integrierbare Kunden-Oberfläche betrieben wird. Zusatzfunktionen wie Berichte, Versandprozesse zum Druck-Provider oder die Integration eines SMS-Gateways lassen sich einfach und schnell mittels standardisierter Web-Services einbinden.

ADMINISTRATION

Zur komfortablen Administration von A²S steht ein webbasiertes Admin-Frontend zur Verfügung. Zusätzlich kann ein eigenes Admin-Frontend auf Basis der ELAXY Web-Services angebunden werden. Darüber können diverse Einstellungen durchgeführt werden. So wird von hier aus auch die funktionale Freigabe im Kunden-Frontend gesteuert.

Folgende Administrations-Services stehen zur Verfügung:

- > System/Systemeinstellungen
- > Mandant/Mandanteneinstellungen/
Aliasarten/Verfahrensarten
- > Kundenkonto/Kundenkonten/Aliaße/
Verfahren/Berechtigungsnachweise
- > Reporting

KUNDEN-FRONTENDS

Das A²S Modul wird ohne eigenes Kunden-Frontend ausgeliefert. Stattdessen können Sie Ihr eigenes Frontend oder Ihre Portaloberfläche durch Web-Service-Schnittstellen flexibel mit dem Modul verbinden.

Folgende Services stehen hier zur Verfügung:

- > Sitzung, z. B. Identifizierung eines Kundenkontos
- > Passwort, z. B. Prüfung eines Passworts, ggf. Sperrung von Passwörtern
- > SMS-TAN/iTAN, z. B. Anforderung und Prüfung einer SMS (i)-TAN oder Ablegen der Transaktionsdaten nach Verbrauch

> iTAN-Block, z. B. Ermittlung aller iTAN Blöcke eines Kundenkontos oder Anforderung eines neuen iTAN Blockes

> Sonstiges (Exporte, Session, Verschlüsselung)

REPORTING

Detaillierte Auswertungen bieten wertvolle Informationen für Management Reports oder Marketinganalysen. In A²S lassen sich verschiedene Auswertungen erzeugen, die wichtige Hinweise auf das individuelle Kundenverhalten im Online-Banking und -Brokerage geben können. Die protokollierten Daten lassen sich anhand von zusätzlichen Grafiktools (u. a. Cognos) über manuelle Exporte weiter veredeln und anreichern.

Beispiele für Auswertungen:

- > Anzahl der Kundenkontos
- > Exporte pro Kundenkonto
- > Sitzungsstatistik

AUTOMATION

Finanzdienstleister können von außen über Web-Services auf automatisierte Abläufe innerhalb von A²S zugreifen. Die Services werden in regelmäßigen zeitlichen Abständen automatisch aufgerufen. Dabei können u. a. neue Passwörter bei Erreichen der Mindestanzahl oder bestimmte Mengen an iTAN-Blöcken für den Druckprozess erzeugt werden. Darüber hinaus lässt sich auch eine Bestätigung über den erfolgreichen Transport verschlüsselter Passwörter an den Druck-Provider realisieren.

MONITORING

A²S ermöglicht das systematische Beobachten, Überwachen und Protokollieren sämtlicher Vorgänge innerhalb des Moduls und Ihrer Prozesslandschaft. Durch entsprechende

Schnittstellen können Sie vorhandene Monitoring-Systeme und -Prozesse integrieren, interne Abläufe effektiv beobachten und steuernd eingreifen, falls Schwellwerte unter- bzw. überschritten werden.

ANBINDUNG AN FREMDSYSTEME

Zum Druck und Versand von PIN- und TAN-Briefen über einen Druck-Provider erzeugt A²S verschlüsselte Rohdaten (PINs, TANs), die über Schnittstellen versandt werden. Die weitere Verarbeitung der Daten wird mit dem Druck-Dienstleister individuell umgesetzt. ■

AUSZUG DER REFERENZEN ELAXY A²S



> Einsatz der ELAXY Authentifizierungs- und Autorisierungslösung



> mehrere Millionen Dokumente für verschiedene Mandanten



> Einsatz der ELAXY Authentifizierungs- und Autorisierungslösung



> Einsatz der ELAXY Authentifizierungs- und Autorisierungslösung



> Zur Authentifizierung und Autorisierung über das Kunden Portal wird ELAXY A²S eingesetzt

> ELAXY A²S – DIE FAKTEN

ELAXY A²S erfüllt, auch unter Berücksichtigung aktueller Diskussionen, alle wesentlichen Aspekte für Online-Sicherheit. Eine Nutzung außerhalb von Banking und Brokerage, z. B. für versicherungsrelevante Vorgänge, ist ebenfalls möglich. Durch die Multi-Mandantenfähigkeit kann A²S auch in einem ASP-Modell betrieben werden.

VERFAHREN

Moderne Verschlüsselungsverfahren (RSH, AES, SHA2) garantieren Ihnen hierbei ein hohes Maß an Schutz vor Internet-Kriminalität. Die Erweiterung um neue TAN-Verfahren, wie z. B. smartTAN Optik ist jederzeit möglich.

→ **PASSWORT** (max. fünf versch. Ausprägungen)

→ **iTAN** (indizierte TAN)

→ **mTAN** (mobile TAN, SMS oder Handy-TAN)

WEB-SERVICES

Unsere Web-Services beschreiben die Möglichkeiten das A²S Modul über entsprechende vordefinierte Services-Klassen hinweg zu administrieren.

→ **ADMIN-FRONTEND**

→ **KUNDEN-FRONTENDS**

→ **REPORTING**

→ **AUTOMATION**

→ **MONITORING**

ANBINDUNG AN FREMSYSTEME

Durch die Einbeziehung externer Systeme ist für Sie als Finanzdienstleister eine durchgehende Leistungskette bis zum Endkunden garantiert (z. B. Druck von PIN Briefen).

→ **DRUCK-PROVIDER**

→ **SMS-GATEWAY**

> ELAXY A²S – DER AUFBAU

Der modulare Aufbau von A²S garantiert ein hohes Maß an Flexibilität. Sie sind jederzeit in der Lage selbst zu bestimmen, welche unterstützenden Anwendungen (Reporting, Frontend, Kundenverwaltung u. a.) Sie benötigen. Die Einbindung des Produkts in Ihre unterschiedlichen Systemlandschaften (Java Technologie) ist problemlos möglich.



ELAXY A²S SUMMARY

LESEN SIE IN DER
AUSGABE 04:
ORDER-
MANAGEMENT

> LEISTUNG

ELAXY bietet Finanzdienstleistern mit dem A2S Modul eine einfach integrierbare, flexibel erweiterbare und kosteneffiziente Lösung zur sicheren Authentifizierung und Autorisierung für Online-Banking- und Online-Brokerage-Plattformen – und schützt damit sicher vor Angriffen aus dem Internet.

> FEATURES

VERFAHREN

- Passwort (max. fünf verschiedene Ausprägungen)
- iTAN (indizierte TAN)
- mTAN (mobile TAN, SMS-TAN)

WEB-SERVICES

- Webbasiertes Admin-Frontend
- Integration eigener Kunden-Frontends
- Reporting
- Automatisierung
- Monitoring

ANBINDUNG AN FREMDSYSTEME

- Druck-Provider
- SMS-Gateway

> HIGHLIGHTS

- Einfache Integration in bestehende System-Umgebungen durch offene Schnittstellen
- Problemlose Erweiterbarkeit um zusätzliche Schutzmechanismen wie elektronische Signaturen oder Zertifikate
- Multi-Mandantenfähigkeit ermöglicht Betrieb als ASP-Modell
- Schlanke Architektur mit minimalen Zugriffszeiten von unter 1 Sekunde
- Aussagekräftige Auswertungen durch integrierte Reporting-Funktionen
- Anreicherung der Auswertungen über externe Reporting-Lösungen
- Einsatzmöglichkeit bestehender Monitoring-Tools zur lückenlosen Überwachung aller Zugriffsaktivitäten
- Maximale Effizienz durch Einrichtung und Steuerung automatisierter Prozesse

> INTERESSIERT?

Gerne stellen wir Ihnen die Funktionen von ELAXY A²S und die individuellen Einsatzmöglichkeiten für Ihren Bedarf näher vor. **Tel.: 09561.5543.0**

Die Inhalte dieses Flyers dienen nur der allgemeinen, nicht abschließenden Information; sie beruhen auf dem Informationsstand zum Zeitpunkt der Veröffentlichung und können sich nach dem Zeitpunkt der Veröffentlichung ohne Ankündigung ändern. Die Inhalte stellen in keiner Beziehung ein Angebot zum Abschluss eines Vertrages dar.

ELAXY Business Solution & Services GmbH & Co. KG

Am Hofbräuhaus 1
96450 Coburg
Germany

Tel. +49 (0) 9561.5543.0
Fax +49 (0) 9561.5543.302
info@elaxy.de, www.elaxy.de



ELAXY

Add Experience