Fragen und Antworten zur Zwei-Faktor-Authentifizierung im Internetbanking

WARUM WIRD EINE ZWEI-FAKTOR-AUTHENTIFIZIERUNG BENÖTIGT?

Die Zwei-Faktor-Authentifizierung muss aufgrund einer delegierten Verordnung der Europäischen Kommission, basierend auf der zweiten Zahlungsdiensterichtlinie (englisch „Payment Services Directive 2“, kurz „PSD2“) – beim Erst-Login, bei Folge-Logins nach 90 Tagen sowie bei der Freigabe von Zahlungsaufträgen erfolgen. Die Abfrage bzw. Überprüfung eines zweiten Faktors dient dazu, die Sicherheit zu erhöhen und eine unautorisierte Verwendung zu verhindern.

Alle von der Bank Austria verwendeten Authentifizierungsverfahren – CardTAN, mobileTAN-SMS und mobileTAN-Push – entsprechen bereits der Zwei-Faktor-Anforderung. Neu ist mit Umsetzung der PSD2, dass auch beim Login ein zweiter Faktor verwendet werden muss.

WELCHE AKTIONEN ERFORDERN EINE ZWEI-FAKTOR-AUTHENTIFIZIERUNG?

Auszug einiger Funktionen, welche eine Zwei-Faktor-Authentifizierung erfordern:

- Erst-Login auf einem neuen Browser

- Folge-Login nach 90 Tagen

- Überweisungsbeauftragung (dabei ist zwingend die Generierung eines einmalig gültigen Authentifizierungscodes vorgeschrieben, der eine dynamische Verknüpfung zum Zahlungsbetrag und dem Zahlungsempfänger aufweist)

WARUM MUSS ICH BEIM LOGIN EINE TRANSAKTIONSNUMMER (=TAN) EINGEBEN?

Aufgrund einer delegierten Verordnung der Europäischen Kommission muss beim Erst-Login sowie bei Folge-Logins nach 90 Tagen eine Zwei-Faktor-Authentifizierung erfolgen. Diese ist bei CardTAN und mobileTAN-SMS durch Eingabe einer TAN durchzuführen.

Tipp für den Browser-Login: Registrieren Sie sich in der MobileBanking App für mobileTAN-Push. Das ermöglicht einen komfortableren Login mit nur einem Klick am Smartphone zur Bestätigung des Logins im Browser.

KANN ICH EINEN LOGIN NICHT AUCH OHNE TAN-EINGABE DURCHFÜHREN?

Aufgrund einer delegierten Verordnung der Europäischen Kommission muss beim Erst-Login sowie bei Folge-Logins im Browser nach 90 Tagen bei CardTAN und mobileTAN-SMS eine TAN für die Zwei-Faktor-Authentifizierung eingegeben werden. Bei Logins in der MobileBanking App muss nach der einmaligen Geräteregistrierung keine TAN mehr eingegeben werden.

Tipp für den Browser-Login: Registrieren Sie sich in der MobileBanking App für mobileTAN-Push. Das ermöglicht einen komfortableren Login mit nur einem Klick am Smartphone zur Bestätigung des Logins im Browser.

WIE ERFOLGT DIE ZWEI-FAKTOR-AUTHENTIFIZIERUNG IM MOBILEBANKING?

Beim Erst-Login in die MobileBanking App wird der User aufgefordert das Gerät (Smartphone oder Tablet) zur Verfügernummer zu registrieren. Die Registrierung erfolgt nach Setzen einer Gerätebezeichnung mittels Bestätigung durch eine TAN. Nach der Registrierung des Geräts stellt dieses den Faktor „Besitz“ dar. Somit wird sichergestellt, dass bei jedem Login in der MobileBanking App mit PIN (Faktor „Wissen“) oder Biometrie (Faktor „Inhärenz“) eine Zwei-Faktor-Authentifizierung erfolgt.

MUSS ICH BEI JEDEM LOGIN IN DIE MOBILEBANKING APP EINE TAN EINGEBEN?

Beim Erst-Login in die MobileBanking App auf einem Smartphone oder Tablet muss für die Registrierung des Geräts eine TAN eingegeben werden. Für jeden weiteren Login auf diesem Gerät ist keine TAN einzugeben.

WIRD BEIM LOGIN SPÄTESTENS NACH 90 TAGEN IN DIE MOBILEBANKING APP EINE TAN VERLANGT?

Eine TAN wird lediglich für den Erst-Login in die MobileBanking App auf einem Smartphone oder Tablet für die Registrierung des Geräts verlangt. Für jeden weiteren Login auf diesem Gerät ist keine TAN einzugeben.

WODURCH UNTERSCHEIDET SICH DER LOGIN IN EINEM BROWSER VON EINEM LOGIN IN DIE MOBILEBANKING APP?

Sowohl im Browser am PC als auch in der MobileBanking App am Smartphone oder Tablet wird beim Erst-Login eine TAN zur Registrierung des Browsers bzw. des Smartphones oder Tablets verlangt.

Nach der Registrierung des Smartphones oder Tablets stellt dieses Gerät den Faktor „Besitz“ dar. Somit wird sichergestellt, dass bei jedem Login in die MobileBanking App mit PIN (Faktor „Wissen“) oder Biometrie (Faktor „Inhärenz“) eine Zwei-Faktor-Authentifizierung erfolgt.

Am PC wird lediglich der Browser registriert, welcher kein physisches Gerät darstellt wie z.B. ein Smartphone oder Tablet. Somit muss beim Folge-Login in einem Browser spätestens nach 90 Tagen erneut eine TAN eingegeben werden. Darüber hinaus werden bei jedem Folge-Login ohne TAN im Browser zahlungsverkehrsbezogene Umsätze und Details maskiert, die älter als 90 Tage sind.

WARUM MUSS BEIM ERST-LOGIN IM BROWSER EIN BROWSERNAME VERGEBEN WERDEN?

Beim Erst-Login in einem Browser sowie bei Folge-Logins nach 90 Tagen muss eine Zwei-Faktor-Authentifizierung erfolgen. Mit der Zwei-Faktor-Authentifizierung beim Erst-Login ist gleichzeitig ein Browsername zu vergeben, sodass dieser Browser eindeutig mit Ihrer Verfügernummer verknüpft wird. Der Browsername wird entsprechend dem verwendeten Browser vorgeschlagen, kann jedoch frei gewählt werden. Aufgrund der Eindeutigkeit der registrierten Browser bzw. Geräte in der Geräteverwaltung Ihres Internetbankings können nicht zwei Browser oder Geräte mit der gleichen Bezeichnung registriert werden. Beim Folge-Login spätestens nach 90 Tagen wird mit der Zwei-Faktor-Authentifizierung die Browserregistrierung bestätigt.

WIE VIELE BROWSER ODER SMARTPHONES BZW. TABLETS KANN ICH REGISTRIEREN?

Die Anzahl der gleichzeitig registrierten Browser oder Geräte ist auf 50 limitiert. Sobald ein weiterer Browser bzw. ein weiteres Gerät registriert wird, wird der Browser bzw. das Gerät mit dem ältesten Login-Datum aus der Liste Ihrer registrierten Geräte in der Geräteverwaltung entfernt.

ICH HABE MEHR ALS EINEN BROWSER AUF MEINEM COMPUTER INSTALLIERT. MUSS ICH JEDEN DIESER BROWSER REGISTRIEREN?

Die Registrierung eines Browsers gilt nicht stellvertretend für alle anderen Browser auf dem gleichen PC oder den Browser des gleichen Herstellers auf einem anderen PC. Somit ist jeder Browser einzeln zu registrieren und mit Ihrer Verfügernummer zu verknüpfen.

WIE FUNKTIONIERT DIE BROWSERREGISTRIERUNG AUS TECHNISCHER SICHT?

Im Zuge der Browser-Registrierung beim Erst-Login wird ein Browser-Cookie auf dem Computer des Users gespeichert. Sowohl das Cookie als auch der gewählte Browsername dienen dazu, den Browser eindeutig mit der Verfügernummer zu verknüpfen, um nach dem Erst-Login für jeden weiteren Login innerhalb von 90 Tagen keine weiteren TANs beim Login eingeben zu müssen.

WAS IST EIN BROWSER-COOKIE?

Laut Wikipedia werden Cookies genutzt, um mit einer Website bzw. Domain verbundene Informationen für einige Zeit lokal auf dem Computer zu speichern und sie dem Server auf Anfrage wieder zu übermitteln.

WAS MUSS ICH BEACHTEN, WENN ICH DIE BROWSER-COOKIES LÖSCHE?

Nach dem Löschen der Browser-Cookies ist die Verknüpfung des Browsers mit Ihrer Verfügernummer nicht mehr gegeben. Daher wird beim nächsten Login auf diesem Browser die Anforderung angezeigt den Browser zu registrieren und so erneut mit Ihrer Verfügernummer zu verknüpfen.

WARUM WERDE ICH BEI JEDEM LOGIN IM BROWSER AUFGEFORDERT DEN BROWSER ZU REGISTRIEREN?

Die Browser-Registrierung erfolgt beim Erst-Login mit dem Setzen eines Browsernamens und der Bestätigung mittels TAN oder mittels Bestätigung via mobileTAN-Push in der MobileBanking App. Sollten Sie bei jedem Login eine Aufforderung erhalten den zuvor zu Ihrer Verfügernummer registrierten Browser erneut zu registrieren, ist der Browser so eingestellt, dass nach dem Schließen des Browsers die Browser-Cookies automatisch gelöscht werden. Um zu vermeiden, dass bei jedem Login die Aufforderung zur Browser-Registrierung erscheint, ist die Cookie-Akzeptanz des Browsers entsprechend einzustellen (z.B. alle Cookies oder nur von bestimmten Seiten akzeptieren). Nähere Infos dazu sind beim Browserhersteller einzuholen.

WARUM IST DIE FUNKTION „ERWEITERTE SICHERHEIT BEIM LOGIN“ NICHT MEHR VERFÜGBAR?

Die Funktion „Erweiterte Sicherheit beim Login“ wurde durch die Implementierung einer Browser-Registrierung ersetzt. Beim Erst-Login in einem neuen Browser wird im Zuge der Browser-Registrierung ein Browser-Cookie auf dem Computer des Users gespeichert. Solange sich das Browser-Cookie auf dem Computer befindet, wird sichergestellt, dass es sich um Ihren Browser handelt. Falls Sie weiterhin bei jedem Login eine TAN eingeben möchten, löschen Sie manuell die Browser-Cookies nach jedem Internetbanking-Logout bzw. stellen Sie sicher, dass die Cookies nach dem Schließen des Browsers automatisch gelöscht werden.

WARUM KANN DIE GERÄTEVERWALTUNG NICHT MEHR DEAKTIVIERT WERDEN?

Die Geräteverwaltung ist erforderlich, um ein Gerät zu registrieren und eindeutig mit der Verfügernummer zu verknüpfen. Dadurch ist eine Zwei-Faktor-Authentifizierung gewährleistet.

WELCHE VORTEILE BIETET MOBILETAN-PUSH GEGENÜBER MOBILETAN-SMS ODER CARDTAN FÜR DIE ZWEI-FAKTOR-AUTHENTIFIZIERUNG IM INTERNETBANKING?

Kunden mit mobileTAN-Push als Zeichnungsmethode bekommen im Zuge der Browser-Registrierung eine Nachricht auf ihrem Smartphone angezeigt und können mittels dedizierter Buttons die Registrierung mit einem Klick bestätigen bzw. ablehnen. Dadurch erübrigt sich das Abtippen einer TAN.

WARUM WERDEN EINIGE ZAHLUNGSVERKEHRSBEZOGENE UMSÄTZE UND DETAILS IM ONLINEBANKING BZW. IN 24YOU MASKIERT ANGEZEIGT?

Bei einem Internetbanking-Folge-Login ohne TAN (OnlineBanking oder 24You) werden zahlungsverkehrsbezogene Umsätze und Details, die älter als 90 Tage sind, maskiert angezeigt. Details maskierter Umsätze können nicht eingesehen, exportiert oder ausgedruckt werden.

WERDEN ZAHLUNGSVERKEHRSBEZOGENE UMSÄTZE UND DETAILS, DIE ÄLTER ALS 90 TAGE SIND, AUCH IN DER MOBILEBANKING APP MASKIERT ANGEZEIGT?

Da beim Erst-Login in die MobileBanking App das Smartphone oder Tablet mit einer TAN registriert wird (Faktor „Besitz“), ist sichergestellt, dass jeder Folge-Login in die MobileBanking App mit PIN (Faktor „Wissen“) oder Biometrie (Faktor „Inhärenz“) einer Zwei-Faktor-Authentifizierung entspricht. Dadurch können zahlungsverkehrsbezogene Umsätze und Details, die älter als 90 Tage sind, im Klartext angezeigt werden.

AUF WELCHE BEREICHE DES INTERNETBANKING BEZIEHT SICH DIE MASKIERUNG DER ANZEIGE DER UMSÄTZE UND DETAILS, DIE ÄLTER ALS 90 TAGE SIND?

Die Maskierung betrifft alle zahlungsverkehrsbezogenen Informationen im Konto-Infobereich (Umsatzliste, Kontoauszüge, e-Kontoauszüge, Valutarische Salden, Export, PFM).

WIE WIRKT SICH DIE MASKIERUNG AUF DIE DETAILANSICHT AUS?

Details maskierter Umsätze können nicht ohne weitere Aktion durch den User eingesehen, exportiert oder ausgedruckt werden.

WIE KANN ICH DIE MASKIERTEN UMSÄTZE UND DETAILS EINSEHEN?

Nach dem Klick auf einen maskierten Umsatz wird eine Aufforderung für die Durchführung einer Zwei-Faktor-Authentifizierung angezeigt. Durch die Durchführung der Zwei-Faktor-Authentifizierung innerhalb der aktuellen Sitzung sind alle Umsätze und Details, die älter als 90 Tage sind, einsehbar und können sowohl exportiert als auch ausgedruckt werden.

WELCHE VORTEILE BIETET MOBILETAN-PUSH BEI DER ANZEIGE VON UMSÄTZEN UND DETAILS, DIE ÄLTER ALS 90 TAGE SIND, IM INTERNETBANKING (ONLINEBANKING UND 24YOU)?

Kunden mit mobileTAN-Push als Zeichnungsmethode bekommen im Zuge der Zwei-Faktor-Authentifizierung für die Anzeige von Umsätzen und Details, die älter als 90 Tage sind, eine Nachricht auf ihrem Smartphone angezeigt und haben die Möglichkeit, diese mittels dedizierter Buttons zu bestätigen bzw. abzulehnen. Dadurch erübrigt sich das Abtippen einer TAN.

WARUM WIRD BEIM ZEICHNEN EINES AUFTRAGS EIN COUNTER ANGEZEIGT?

Ab dem Zeitpunkt der Anforderung einer TAN für eine Überweisung haben Kunden 5 Minuten Zeit auf den Button „Unterschreiben“ zu klicken, bis die Sitzung beendet wird. Nach 4 Minuten erscheint eine Counteranzeige der verbliebenen Sekunden, beginnend mit 00:59.

WARUM MUSS FÜR MULTI BANKS STANDARD (MBS) EIN NEUES SICHERHEITSZERTIFIKAT ANGELEGT WERDEN?

Für jeden Kommunikationsberechtigten muss im Zuge der „PSD2 Strong Customer Authentication“ ein neues Sicherheitszertifikat generiert und mittels TAN gezeichnet werden. Bei der Generierung werden ein privater Schlüssel und ein Sicherheitszertifikat erstellt, welche dem Kommunikationsberechtigten zugewiesen werden und nur von diesem verwendet werden können.

WIE LANGE IST DAS SICHERHEITSZERTIFIKAT GÜLTIG?

Das Zertifikat ist 20 Jahre lang gültig.

WAS IST DER NUTZEN DES SICHERHEITSZERTIFIKATES?

Mit der doppelten Authentifizierung wird der Zeitraum von 90 Tagen für die „MBS-Strong Customer Authentication“ nicht mehr benötigt, somit muss für die Abfrage von Kontoinformationen, die älter als 90 Tage sind, keine TAN mehr eingegeben werden.

WARUM MUSS IM MBS-BEREICH BEI JEDER MOBILETAN-ANFORDERUNG DIE PIN EINGEGEBEN WERDEN?

Hier erfolgt eine Zwei-Faktor-Authentifizierung, welche den Anforderungen des „Zahlungsdienstegesetzes 2018“ (ZaDiG 2018) unterliegt. Demgemäß muss aus Sicherheitsgründen bei jeder MobileTAN-Eingabe auch die PIN eingegeben werden.

MUSS IM MBS-BEREICH MIT JEDER CARDTAN-ANFORDERUNG DIE PIN EINGEGEBEN WERDEN?

Aufgrund der Vorgaben von ZaDiG 2018 ist auch beim CardTAN-Verfahren eine Zwei-Faktor-Authentifizierung notwendig. Sie wird so umgesetzt, dass die Anforderung einer CardTAN durch Eingabe der PIN am CardTAN-Generator erfolgt.