

## Ihr Sicherheitsvorteil gegenüber Betrug beim Onlinebanking

Online-Banking hat sich als eine bei Bankkunden beliebte Dienstleistung erwiesen, da es den jederzeitigen Zugang zu Bankdienstleistungen ermöglicht. Die Zunahme bei immer kreativer ausgeführten Onlinebanking-Betrugsdelikten und bei aufsehenerregenden Identitätsdiebstahlsangriffen kann jedoch das Vertrauen der Verbraucher in Online-Dienstleistungen schnell untergraben.

Neue Sicherheitsvorkehrungen, wie Token, gegenseitige Authentifizierung, Einmalpasswörter und Verbraucheraufklärung haben sich als erfolgreiche Abschreckungsmittel gegen herkömmliche Betrugsfälle, einschließlich Phishing-Angriffe, bewährt. Jedoch kann der bestehende Schutz beim Onlinebanking bei raffinierteren Diebstählen, wie z. B. „Man in the Middle (MitM)“ (Mann in der Mitte) - und „Man in the Browser (MitB)“ (Mann im Browser)-Attacken oftmals umgangen werden.

Die gute Nachricht ist, dass die fortschrittlichen Merkmale von WWS Mobile Security ein bewährtes und effektives Abschreckungsmittel gegen bestehenden und neu auftretenden Betrug beim Onlinebanking und Identitätsdiebstahl bereitstellen. WWS Mobile Security ist eine Mobile APP, die fehlerfrei auf den wichtigsten Smartphone-Betriebssystemen funktioniert und zur Verbesserung der Sicherheit und Senkung der Betriebskosten mühelos in die bestehende Infrastruktur einer Bank integriert werden kann.

Mit WWS Mobile Security können Kunden bequemen Zugriff auf ein hochsicheres Instrument mit einer Authentifizierung über einen zweiten Kanal erhalten, welcher ihnen:

- ✓ *größere Sicherheit bei der Authentifizierung beim Zugriff auf ihr Onlinebanking*
- ✓ *größere Sicherheit bei der Autorisierung von Zahlungsanweisungen oder bei der Verwaltung ihrer Einstellungen im Sicherheitsprofil bietet.*

### Warum sollte WWS Mobile Security verwendet werden?

#### **WWS Mobile Security bedeutet stärkere Sicherheit und Kontrolle**

WWS Mobile Security stellt alle Vorzüge eines Sicherheitstoken für dedizierte Hardware bereit, jedoch ohne die zusätzlichen Kosten. Außerdem funktioniert WWS Mobile Security auf dem Smartphone des Kunden, so dass es nicht erforderlich ist, ein weiteres Gerät mit sich zu führen. Allerdings sind geringere Kosten und mehr Kundenkomfort nicht die einzigen Vorteile. WWS Mobile Security bietet ebenfalls höhere Sicherheitsvorteile gegenüber herkömmlichen Hardware-Sicherheitstoken. WWS Mobile Security zeigt beispielsweise auch bei der Autorisierung einer Zahlungsanweisung detaillierte Informationen über das Internet-Service-Account und die autorisierten Zahlungsdetails an. Durch das Überprüfen aller Zahlungsdetails genießt der Kunde ein größeres „Rundum-sorglos-Gefühl“ und das Risiko fehlerhafter Transaktionen wird deutlich verringert.

#### **Einfache Integration in die bestehende Bankeninfrastruktur**

Die sicheren Authentifizierungsmerkmale von WWS Mobile Security können problemlos zu jedem Internetbanking-System hinzugefügt werden, um die bestehenden Sicherheitsoptionen zu ergänzen und zu verstärken. WWS Mobile Security beinhaltet ebenfalls einen Aktivierungsprozess mit Anleitung für die Kunden, worin anschaulich erklärt wird, wie sie ihre WWS Mobile Security-APP in wenigen einfachen Schritten registrieren können und ihnen die Vorteile und die Nutzung der APP für maximalen Schutz und Komfort aufgezeigt werden.

## Bequem und einfach anzuwenden

Eine stückweise Reaktion auf Bedrohungen für das Onlinebanking kann leicht eine unüberschaubare und schwierige Kundenerfahrung zur Folge haben. Die Design-Philosophie von Auriga besteht darin, die Sicherheit zu verstärken und gleichzeitig Verbraucherfreundlichkeit und Bedienkomfort zu fördern.

Folglich wurde WWS Mobile Security für die intuitive Nutzung entwickelt und nutzt die immer beliebtere QR-Code-Technologie. QR-Codes sind heutzutage alltäglich und von Smartphone-Nutzern weitgehend anerkannt und akzeptiert. Daraus folgend übernehmen Kunden in zunehmendem Maße WWS Mobile Security als sicheres und bequemes Banking-Tool. Das Hinzufügen der starken Authentifizierung von WWS Mobile Security zu Ihrem Onlinebanking-System gewährleistet maximalen Schutz vor Angriffen und höchste Verbraucherfreundlichkeit.



## Weshalb ist WWS Mobile Security sicher?

WWS Mobile Security verwendet einen hoch verschlüsselten Kommunikationskanal zwischen der Telefonanwendung und dem Server, basierend auf dem Industriestandard-SSL-Protokoll und proprietären Sicherheitsalgorithmen. Jede von WWS Mobile Security verwendete Nachricht wird mit einem MAC (Message Authentication Code - Nachrichtenauthentifizierungscode) gekennzeichnet und mittels eines OTP-Passworts (Einmalpasswort) verschlüsselt. Dieses Passwort wird durch ein Hardware-Sicherheitsmodul (HSM) generiert, um höchste Sicherheitsstandards zu gewährleisten. Der MAC basiert auf proprietären Algorithmen und wird bei jeder Transaktion zwecks bestmöglicher Nachrichtenintegrität und Sicherheit neu generiert.

Zusätzlich zu den robusten Verschlüsselungstechniken wirkt WWS Mobile Security auch MitM/MitB-Attacken entgegen, indem dem Kunden vom Internetbanking-System abgerufene Echtzeit-Informationen mittels Nutzung eines zweiten, unabhängigen Kanals angezeigt werden. Kunden können die Genauigkeit der Informationen mühelos sowohl auf ihrem Internetbanking-Kanal, als auch auf dem Mobile-Kanal überprüfen, um sicherzustellen, dass Manipulationen von Informationen nicht unentdeckt bleiben.



## Wie funktioniert WWS Mobile Security?

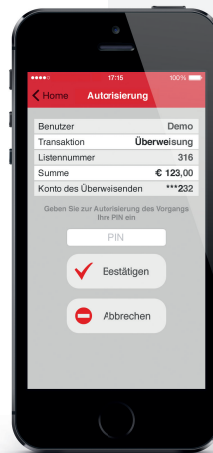
1



### Zugriff auf Ihr Onlinebanking-Konto

Nach der Eingabe Ihrer Onlinebanking-Benutzer-ID und des Passworts wird ein einmaliger QR-Code auf Ihrem Onlinebanking-Bildschirm angezeigt. Starten Sie zur Erfassung des QR-Codes einfach die WWS Mobile Security-APP auf Ihrem Telefon und geben Sie Ihre WWS Mobile Security-PIN ein, um den Authentisierungsprozess abzuschließen.

2



### Autorisierung der Zahlungsanweisungen

Nach Bestätigung der auszuführenden Transaktionsdaten müssen Sie nur noch die WWS Mobile Security-APP auf Ihrem Smartphone starten, um den von Ihrem Onlinebanking-System angezeigten QR-Code zu erfassen. Überprüfen Sie, dass die von WWS Mobile Security angezeigten Zahlungsanweisungen mit Ihrer Onlinebanking-Eingabe übereinstimmen und autorisieren Sie dann die Zahlung mittels Verwendung Ihrer WWS Mobile Security-PIN.

#### Hauptsitz - Bari

Strada Vassallo, 1  
70125 Bari  
Italien  
Tel.: +39.080.5692111  
Fax: +39.080.5692112  
headquarters@aurigaspa.com

#### Standort Mailand

via Santa Maria Valle, 3  
20123 Milano  
Italien  
Tel.: +39.02.00681.583  
Fax: +39.02.00681.400  
milan@aurigaspa.com

#### Standort Rom

via R. Gigante, 20  
00143 Roma  
Italien  
Tel.: +39.080.5692111  
Fax: +39.080.5692112  
rome@aurigaspa.com

#### Standort London

Building 3, 566 Chiswick High Road  
W4 5YA London  
Vereinigtes Königreich  
Tel.: +44 (0)208 849 8022  
Fax: +39.080.5692112  
london@aurigaspa.com

#### Standort Paris

18 rue Pasquier  
75008 Paris  
Frankreich  
Tel.: +33 (0)1.78.41.40.87  
Fax: +33.(0)1.78.41.44.40  
paris@aurigaspa.com

#### Standort Frankfurt

Taunusanlage 1  
60326 Frankfurt  
Deutschland  
Tel.: +49 69 50 50 60 702  
Fax: +49 69 50 50 60 520  
frankfurt@aurigaspa.com