ضوابط خدمة الرموز التفاعلية القصيرة عبر الهاتف المحمول (USSD)

التاريخ: 31 مارس 2026م

النمرة: ب س م/ إ ع ت ت ج م/ إ ش م/ 2026

الموافق: 12 شوال 1447 هـ

الإدارة العامة لتنظيم وتنمية الجهاز المصرفي

منشور رقم (7/2026)

معنون لكافة المصارف والمؤسسات المالية ومقدمي خدمات الدفع الإلكتروني

الموضوع: ضوابط خدمة الرموز التفاعلية القصيرة عبر الهاتف المحمول (USSD)

في إطار جهود البنك المركزي لتعزيز الشمول المالي وتطوير البنية التحتية للمدفوعات الرقمية وعملاً بأحكام قانون تنظيم العمل المصرفي لسنة **2004م** و المادة **6-و** من قانون بنك السودان المركزي لسنة **2002م** تعديل **2012م**، وإستناداً الى لائحة تنظيم أعمال نظم الدفع لسنة **2013م** و لائحة تنظيم وترخيص المؤسسات المالية للدفع عبرالموبايل لسنة **2020م** يصدر بنك السودان المركزي ضوابط وموجهات لتنظيم خدمة الرموز التفاعلية عبر الهاتف المحمول **USSD** (Unstructured Supplementary Service Data - والتي تهدف إلى توفير قناة دفع آمنة سهلة الوصول، منخفضة التكلفة للفئات التي لا تتوفر لديها خدمات الإنترنت أو الهواتف الذكية.

وتمثل هذه الضوابط الحد الأدنى الواجب الإلتزام به على النحو التالي:

أولاً: التعريفات:

البنك	يقصد به بنك السودان المركزي.
خدمة **USSD**	هي تقنية اتصال فورية بدون انترنت عن طريق إدخال رموز قصيرة في الهاتف الجوال تسمح للمستخدم بالتفاعل مع خدمات مصرفية مختلفة عبر شبكات شركات الإتصالات.
شركات الاتصالات	الشركات المصرح لها بالعمل بالسودان من جهاز تنظيم الإتصالات والبريد (**TPRA**) وتقدم خدمات الإتصالات السلكية واللاسلكية والإنترنت والحلول التقنية.
المؤسسات المالية للدفع عبرالموبايل	الشركات التي تحصلت على ترخيص من بنك السودان المركزي على تقديم خدمات الدفع عبرالموبايل بموجب لائحة ترخيص وتنظيم أعمال المؤسسات المالية للدفع عبرالموبايل لسنة 2020م.
مقدمي خدمات الدفع الإلكتروني	يقصد بها أي جهة مرخص لها من قبل البنك لتقديم خدمة دفع.
العميل/المشترك	الشخص المسجل للاستفادة من خدمات الهاتف المحمول الخاصة بالخدمات المالية الرقمية.
البيانات الشخصية	أي معلومات تتعلق بشخص طبيعي محدد أو قابل للتحديد، وفقاً لقانون حماية البيانات.
OTP	كلمة مرور تستخدم لمرة واحدة فقط (**one time password**)
المصادقة الثنائية **2FA**	وسيلة أمان إضافية لحماية الحسابات الإلكترونية (**two factor authentication**)
IMSI	رقم تعريف المشترك في شركة الإتصالات
IMEI	رقم تعريف الهاتف المحمول

MSISDN	رقم الهاتف المحمول (المعرف الفريد المستخدم في شبكات الإتصالات لتحديد المشترك)

ثانيا : الضوابط التنظيمية:

- **السلطات التنظيمية**

1. يختص البنك بالإشراف على الخدمات المالية الرقميةوعلى جميع مقدمي الخدمات المالية عبر قناة USSD الحصول على الموافقة قبل إطلاق الخدمة.
2. تتولى شركات الإتصالات تخصيص الرموز القصيرة لخدمة USSD وفقاً للوائح جهاز تنظيم الإتصالات والبريد.

- **نطاق الخدمة**

ينظم هذا المنشور خدمة الرموز التفاعلية (USSD) بوصفها قناة وصول إلى الخدمات المالية الرقمية الخاضعة للتنظيم ، وتُعد مكمّلة للضوابط والموجهات ذات الصلة بنظم الدفع وفي حالة وجود اي تعارض تسود أحكام قانون بنك السودان المركزي لسنة 2002م تعديل 2012م.

يسمح بإستخدام (**USSD**) لتقديم الخدمات المصرفية التالية:

1. فتح حسابات محافظ إلكترونية (وفق السقوفات التي يحددها البنك)
2. التحويلات المالية
3. المدفوعات الحكومية
4. دفع الفواتير
5. الإستعلامات المالية
6. المدفوعات التجارية

ج- الجهات المسموح لها تقديم الخدمة

1. المصارف
2. المؤسسات المالية للدفع عبر الموبايل
3. مقدمي خدمات الدفع الإلكتروني

د- متطلبات الموافقة على الخدمة

1. إتفاقية بين المصرف وإحدى شركات الإتصالات المرخصة العاملة بالبلاد.
2. شهادة الترخيص للمؤسسات المالية للدفع عبرالموبايل ومقدمي خدمات الدفع الإلكتروني من البنك.
3. ملء إستمارة تقديم الخدمة موقعة ومختومة من الجهة طالبة الترخيص.
4. شهادة الإختبارات الفنية للخدمة والربط بين انظمة مقدم الخدمة وشركة الإتصالات.
5. خطة إدارة المخاطر والتعافي من الكوارث.
6. مقترح للمصاريف والرسوم لكل خدمة مقدمة.
7. وصف إجراءات العناية الواجبة للعملاء التي تطبق عند فتح المحافظ الإلكترونية.

ثالثا: ضوابط استخدام خدمات USSD:

- **إدارة الجلسة**

1. يجب على مقدم الخدمة تخصيص معرف فريد لكل جلسة دخول وإنهاء الجلسة بعد 30 ثانية من الخمول ومنع إعادة استخدام أو إعادة إرسال رسائل الجلسة. كما يجب إظهار شاشة تأكيد للعمليات بصيغة تأكيد العملية نعم/لا .
2. يجب التنبيه في حالة تكرار العملية بنفس المبلغ.

- **إدارة الأخطاء**

1. يجب إرسال رسالة واضحة عند فشل المعاملة.
2. يجب عدم الخصم من الرصيد عند فشل المعاملة.
3. إعادة المحاولة الآمنة بحد اقصى ثلاثة محاولات.

ج- الإشعارات (إشعار إلكتروني)

1. يجب ارسال إشعار في حالة نجاح او فشل العملية.
2. يجب ان تحتوي الرسالة على رقم مرجعي.
3. يجب إرسال رسالة نصية قصيرة (SMS) مجانية فور اكتمال العملية توضح التفاصيل (المرسل،المستفيد،المبلغ،التاريخ،تاريخ انتهاء المعاملة، الرقم المرجعي).

د- آلية إلغاء الخدمة

1. يجب توفير خاصية إيقاف الخدمة عبر رمز ضمن قائمة الخدمات المتاحة للمستخدم.
2. يجب توفير آلية لإيقاف الخدمة عبر مركز او رقم إتصال موحد.
3. اتاحة إيقاف الخدمة عبر المصرف.

ه- إدارة المنازعات (Dispute)

1. يجب تقديم الدعم الفني على مدار الساعة
2. يجب تسجيل كافة المعاملات والإحتفاظ بها وفق مايحدده البنك.
3. يجب حل الشكاوي خلال فترة بحد أقصى 48 ساعة (أو كما يحددها البنك)
4. يجب توفير آلية لحل المنازعات مع مراعاة الضوابط المنظمة للعمل المصرفي.

و- حماية المستهلك والتوعية الأمنية:

1. يجب الإفصاح عن الرسوم وأن تظهر رسالة للمستخدم توضح قيمة الرسوم لكل رمز تفاعلي.
2. يجب إرسال رسائل نصية (SMS) تحذيرية دورية للعملاء ضد الاحتيال.
3. يجب توفير مركز دعم فني (Call Center) مخصص للبلاغات الطارئة والشكاوى المالية.
4. يجب إخفاء بيانات الحساب الحساسة (Masking) في واجهة خدمة الرموز التفاعلية.

ز- الرقابة وإدارة التقارير:

1. يلتزم المصرف ، المؤسسة المالية، مقدم خدمة الدفع بتقديم تقرير دوري يشمل (حجم العمليات، الفشل التقني، محاولات الاحتيال) في اليوم الخامس من كل شهر لادارة نظم الدفع ببنك السودان المركزي.
2. يجب الإحتفاظ ببيانات العمليات وسجلات المراجعة لمدة خمسة سنوات لأغراض التدقيق.
3. يجب إعداد خطط الطوارئ واستمرارية الأعمال.
4. تخضع الخدمة لرقابة وتفتيش البنك وعلى مقدم الخدمة تمكين البنك من الوصول الى كافة البيانات والتقارير والمعلومات المطلوبة وتقديمها.
5. يجب على مقدم الخدمة تفعيل أنظمة لمراقبة الإحتيال و رصد الأنماط غير الإعتيادية مثل التكرار المرتفع على نحو غير معتاد وأنماط استبدال الشريحة وتعدد تغييرات الأجهزة.

ح- التشغيل البيني ومعايير الربط والإتصال

1.الربط بالمحول القومي المركزي : يلتزم جميع مقدمي خدمات الدفع بربط منصات USSD الخاصة بهم بالمحول القومي المركزي، متى كان متاحاً، بما يحقق قابلية التشغيل البيني للأموال.

2.معايير الواجهات البرمجية: ينبغي أن تلتزم المصارف والمؤسسات المالية و مقدمي خدمات الدفع بمعيار واجهة برمجة تطبيقات الأموال عبر الهاتف المحمول الصادر عن GSMA (الإصدار 2.0 أو ما بعده) أو أي معايير مكافئة، وذلك فيما يتعلق بالإستعلام عن الحسابات والمدفوعات. كما يجب أن تستخدم الرسائل

المتبادلة بين مقدمي خدمات الدفع والمصارف صيغاً معيارية مثل ISO 8583 أو ISO 20022 متى كان ذلك منطبقاً.

3.معايير الاتصالات: يجب أن يتوافق استخدام خدمة USSD مع المواصفات الفنية الصادرة عن 3GPP/ETSI مثل 3GPP TS 23.090 فيما يتعلق بتسلسل الرسائل وتدفقها ويقع على عاتق مقدمي خدمات الدفع مسؤولية ضمان توافق سلوك التطبيق مع هذه المعايير.

رابعا: ضوابط مكافحة غسل الأموال وتمويل الإرهاب (AML/CFT)

1. يجب أن تمتلك أنظمة مقدمي خدمة USSD القدرة على رصد المعاملات المشبوهة.
2. يجب تحليل حجم وتكرار المعاملات.
3. يجب الابلاغ عن المعاملات المشبوهة.
4. العناية الواجبة تجاه العملاء (KYC/CDD)
5. التسجيل المسبق: يحظر تفعيل خدمة التحويل عبر USSD لأي عميل لم يستوفِ بيانات اعرف عميلك (KYC) كاملة ومحدثة في النظام المصرفي الأساسي.
6. ربط الهوية بالهاتف: يجب التأكد من أن رقم الهاتف المستخدم في الخدمة مسجل باسم العميل لدى شركة الاتصالات وبموجب الهوية الوطنية (SIM-ID Mapping).
7. المستويات المتدرجة: تطبيق مبدأ العناية الواجبة المبسطة (Simplified CDD) للعمليات الصغيرة والعناية المشددة (Enhanced CDD) للعمليات التي تقترب من السقوف العليا.
8. مراقبة العمليات والأنماط المشبوهة وإبلاغ البنك عنها.
9. المراقبة اللحظية: يجب أن يمتلك المصرف نظاماً آلياً (AML Monitoring System) قادراً على رصد الأنماط التالية عبر قناة USSD:

9.1 التجزئة (Structuring): تقسيم المبالغ الكبيرة إلى عمليات صغيرة متعددة لتفادي السقوف الرقابية.

9.2 التدفق السريع (Velocity Checks): رصد الحسابات التي تستقبل تحويلات عديدة من أطراف مختلفة وتفرغها فوراً.

9.3 الخمول المفاجئ: تنشيط حسابات كانت خاملة لفترات طويلة وبدء عمليات تحويل مكثفة عبر قناة USSD.

9.4 القوائم السوداء والحظر.

9.5 الفحص الفوري: يجب ربط نظام التحويل بقوائم الحظر المحلية والدولية (Sanction Lists) لمنع أي تحويل صادر أو وارد لأسماء مدرجة في قوائم الإرهاب أو المحظورين.

9.6 تجميد العمليات: يلتزم المصرف بتجميد أي عملية مشبوهة فوراً وإخطار البنك خلال 24 ساعة.

9.7 تصنيف المخاطر: تصنيف عملاء خدمة USSD إلى فئات (منخفض، متوسط، مرتفع المخاطر) بناءً على المهنة، الموقع الجغرافي، وحجم المعاملات المعتاد وأي معايير يراها المصرف ملائمة ثم تعديل سقف التحويل آلياً بناءً على هذا التصنيف.

خامسا : الضوابط الفنية

- **المصادقة والأمن**

1. تتطلب جميع المعاملات التي تُباشر عبر خدمة USSD استخدام الرقم السري للعميل أو رمز مصادقة آمن.
2. إدخال الرقم السري بصورة مشفرة/مخفية مع حظر تخزينه أو تسجيله بصيغة نصية مكشوفة.
3. تعليق الاستخدام بعد ثلاث محاولات متتالية فاشلة لإدخال الرقم السري بحيث لا تتم إعادة الضبط إلا من خلال المصرف أو مركز الاتصال.
4. المصادقة الثنائية (2FA) لكافة المعاملات ذات القيمة الكبيرة . ويجوز لمقدمي خدمات الدفع استخدام وسائل تحقق خارجية مستقلة عن جلسة USSD مثل الرسائل النصية لمرة واحدة (OTP) أو المكالمة الصوتية أو تطبيقات المصادقة شريطة أن تكون محمية بضوابط التحقق من استبدال شريحة SIM .

5. ربط الجهاز يجب على مقدمي خدمات الدفع استخدام عنصرين على الأقل من العناصر الآتية للتحقق من صحة الجلسة (IMSI أو IMEI) أو الطابع الزمني لاستبدال شريحة SIM أو تاريخ إعادة تخصيص رقم الهاتف (MSISDN recycling date) أو الطابع الزمني لتغيير الجهاز ويقتصر استخدام هذه البيانات على أغراض منع الاحتيال.

- **التشفير :**

1. **تشفير النقل**: يجب على مشغلي شبكات الهاتف المحمول ومقدمي خدمة الرموز التفاعلية تأمين جميع روابط رسائل USSD باستخدام بروتوكول TLS 1.2 أو أعلى مع التحقق المتبادل من الهوية واستخدام خوارزميات تشفير قوية، كما يجب أن تستخدم جميع الواجهات البرمجية الداخلية بين بوابات USSD والأنظمة الخلفية قنوات مشفرة.
2. **التشفير والتعامل مع البيانات**: يجب تشفير جميع بيانات العملاء بما في ذلك البيانات الشخصية وتفاصيل المعاملات أثناء النقل وأثناء التخزين ويلتزم مقدم الخدمة بمعايير ISO/IEC 27001 فيما يتعلق بإدارة المفاتيح وضوابط الأمن ولا يجوز تضمين البيانات الحساسة مثل الأرقام السرية أو رموز التحقق لمرة واحدة ضمن محتوى رسائل USSD إلا في الحدود اللازمة للمصادقة.

ج- الشفافية:

1. يحظر عرض أي بيانات حساسة (مثل الرصيد الكامل أو رقم الحساب كاملاً) في رسائل الاستجابة.
2. **د- حدود العمليات المالية**:

1- يحدد السقف اليومي بمبلغ خمسمائة الف جنيه سوداني فقط (**500**,**000**) وللبنك الحق في تعديلها حسب مقتضيات المخاطر ومتطلبات تقديم الخدمة وذلك بالتنسيق مع المصارف والمؤسسات المالية ومقدمي خدمة الدفع.

سادسا: ضوابط وأحكام عامة

1. تقتصر الخدمة على المصارف و المؤسسات المالية للدفع عبرالموبايل المرخصة ومقدمي خدمات الدفع الإلكتروني.
2. لاتمنح رخصة مستقلة لخدمة USSD بل تتم الموافقة ضمن خدمات المصارف والمؤسسات المالية للدفع عبرالموبايل ومقدمي خدمات الدفع الإلكتروني.
3. يجب التأكد من هويات العملاء وملكية رقم الهاتف المحمول.
4. يجب عدم مشاركة بيانات العملاء لأي جهة إلا بعد الحصول على موافقة البنك.
5. يجب الإلتزام التام بالسقوفات التي يحددها البنك.
6. يجب توفير التقنيات والإعدادات الفنية اللازمة للربط البيني بين المصارف .
7. يجب الإلتزام بتطبيق قواعد ومتطلبات مكافحة غسل الأموال وتمويل الإرهاب.
8. يجب تطبيق الإجراءات التي تعزز الثقة في الخدمة وحماية المستهلك.
9. يجب إدارة المخاطر المختلفة والمتوقعة وفي حالة تغير ملكية رقم الهاتف يجب قفل المحفظة وإخطار العميل وكذلك مخاطر فقدان الهاتف المحمول.
10. يجب على المصرف/ المؤسسة المالية/ مقدم خدمة الدفع الإلكتروني توقيع اتفاقية مستوى الخدمة (SLA) مع شركات الإتصالات تضمن استمرارية الخدمة بنسبة لا تقل عن 99.9% وسرعة استجابة لا تتعدى ثوانٍ معدودة.
11. يجب تخصيص رمز USSD موحد (Short Code) لكل مقدم خدمة لسهولة التعرف عليه من قبل العملاء ومنع الإحتيال.

تسري هذه الضوابط إعتباراً من تاريخه وعلى المصارف والمؤسسات المالية ومقدمي خدمات الدفع الإلكتروني الإلتزام بما ورد في هذا المنشور قبل إطلاق الخدمة. ويحق للبنك إتخاذ الإجراء المناسب في حالة المخالفة.

ع/ بنك السودان المركزي

ياسر عبدالرحمن الياس د.الفاتح النور الحسن

إدارة الشئون المصرفية

الإدارة العامة لتنظيم وتنمية الجهاز المصرفي