Most Money External ProtocolSpecification

(Protocol definition for External Institutions & Terminals)

МОСТ ПСП ХХК
2017

АГУУЛГА

1. ХҮСЭЛТ ДАМЖУУЛАХ СУВАГ

Гадны хост болон терминалууд МОСТ-ын систем рүү HTTPS протоколоор холбогдож хүсэлт илгээнэ.HTTPS протоколоор холбогдохдоо X509 стандартын сертификаттай байх ба ServerAuthentication болон ClientAuthentication хийнэ. Сертификатуудыг МОСТ-оос олгоно. X509 сертификатын нийтийн түлхүүрийн урт багадаа 1024 бит байна.

2. ХҮСЭЛТИЙН БҮТЭЦ

Хүсэлт нь толгой буюу HTTP header дээрх утгууд болон бие буюу HTTP body –с бүрдэнэ.
Толгой хэсэгт протоколын хувилбар, уг хүсэлтийн төрөл зэргийг агуулна.
Бие хэсэгт хүсэлтийн үндсэн параметрүүдийг агуулах ба JSON форматтай байна.

Толгой болон бие хэсгийн параметрүүд нь дараах төрөлтэй байна:

N	тоон утгатай талбар
ANS	үсэг тоо, тусгай тэмдэгээс бүтсэн текст
HEX	16 –тын бүтэцтэй утга

Талбарын уртыг тодорхойлохдоо дараах форматуудыг ашиглана:

N5	5 цифрээс бүрдсэн тоо
N..5	5 хүртэлх цифрээс бүрдсэн тоо
ANS..16	16 –с уртгүй текст

Header буюу толгой хэсгийн параметрүүд:

Header Field Name	Tag	Value	Field Format	Mandatory
ProtocolVersion	**PV**	05– MAPI+ version	N2	M
Transaction Type	**TT**	6-р бүлгээс харна уу	N4	M
RejectStatus	**RS**	00 – for standart messages 99 – for reject messages Хүсэлтийг хүлээн авагч тал хүсэлтийн бие хэсгийг тайлж уншиж чадаагүй бол 99 гэсэн утга анхны хүсэлтийн энэ талбартсолиж буцаана.	N2	M

Бие буюу үндсэн хэсгийн параметрүүд:

Body Field Name	Tag	Value	Field Format
secureData	**SD**	Терминал дээрээс нууцлах шаардлагатай талбаруудыг багцалж (JSON форматтай) нууцлалын алгоритмаар хувиргасан үр дүн. */Нууцлах талбаруудыг 5-рбүлгийн хүснэгтэд *-р тэмдэглэсэн, нууцлалын алгоритмыг 7 бүлгээс харна уу./*	ANS
EncryptedOneTimeKey	**EK**	Нууц талбарыг задлах нэг удаагийн түлхүүр.	ANS

		/Нууцлалын алгоритмыг 7 бүлгээс харна уу./	
Singature	**SG**	Нууцлагдсан утгууд өөрчлөгдсөн эсэхийг шалгах Гарын үсэг. */Нууцлалын алгоритмыг 7 бүлгээс харна уу./*	ANS
OtherFields		Бусад гүйлгээний талбарууд. */Талбаруудыг 8-рбүлгээс харна уу./*	

3. ТАЛБАРЫН ЖАГСААЛТ

Field	Type	Description
billId	ANS…20	Биллийн дугаар
channel	N..2	Гүйлгээнийсуваг 44–External Terminal&Host
deviceIP	ANS..100	Терминал төхөөрөмжийн IP
deviceMac	ANS..100	Терминал төхөөрөмжийн MAC
deviceName	ANS..100	Терминал төхөөрөмжийннэр
isCheckQr	N1	Хүсэлтийн төрөл 0-QR төлбөр шалгах, 1-QR төлбөр цуцлах
lang	N1	Хэл 0-Монгол, 1-Англи
payeeId	N..10	QR кодүүсгэж байгаа мерчант дугаар
posNo	N..20	QR кодүүсгэж байгаа мерчантын терминалын дугаар
qrAccountNumber*	ANS..30	QR код холбох дансны дугаар
qrAccountName	ANS..200	QR код холбох дансны нэр
qrBankCode	ANS..6	Дансны банкны дугаар
qrCode*	ANS50	QR код
refNo	ANS…12	ТАН-тай худалдан авалтын гүйлгээний рефренс дугаар
srcInstId	ANS..20	Шилжүүлэх болон хүсэлт илгээж буй СБ-н дугаар
srcMsisdn*	N8	Худалдан авагчийнутасныдугаар
tan*	N6	Худалдан авагчийн нэг удаагийн гүйлгээний нууц дугаар
traceNo**	N16	Гүйлгээнийтрэйсдугаар. Тухайнхостынхувьддахиндавтагдашгүйдугаарбайх бөгөөд тэмдэгтийн хэмжээ нь 16 байх ёстой.

tranAmount	N..12	Гүйлгээнийдүн
tranCur	ANS3	Гүйлгээнийвалют Валютын жагсаалтаас сонгоно. ХудалданавалтынгүйлгээндээрбайнгаMNTбайна. Аквайрершимтгэлийнвалютньгүйлгээнийвалюттайижил байна.
tranDesc	ANS..60	Гүйлгээнийутга. Терминалаасгүйлгээнийутгаөгчболно. ЭнэутганьМостэсвэлбанкнысистемийндансныхуулгадээрхарагдана.
vatUserNo	ANS8	НӨАТУС-н хэрэглэгчийн дугаар

** Тэмдэглэгээтэй талбаруудыг нууцалж дамжуулна.*
*** traceNo– Трэйсийн дугаарын хувьд сүлжээний холболт шалгах хүсэлт дээр нууцлалгүй дамжуулна.*

4. ГҮЙЛГЭЭНИЙ ТӨРӨЛ

API руу хүсэлт илгээхдээ URL хаягийн ард "/TT" тэмдэгт болон гүйлгээний төрлийн кодыг залгана. Жнь (QR үүсгэх): https://webpos.merchant.mn/ots/api/mapi/**TT3061**

"TT" талбарын кодыг дараах хүснэгтэд тодорхойлов.

Transaction Type	Description
Financial transactions	
1608	ТАН-тай худалдан авалт
3051	Худалдан авалтын QR үүсгэх
3065	QR кодоортөлбөр лавлах(нэг QR код)

5. RESPONSE КОД

"responseCode" талбарын утга дараах хүснэгтээр тодорхойлогдоно. Энэхүү хүснэгт нь нэмэгдэж өөрчлөгдөх боломжтой.

ResponseCode	Description
0	Гүйлгээ амжилттай.
7000	Системдалдаагарлаа.
7001	
7002	Холболттасарсанбайна! Тадахиннэвтэрнэүү.
7003	Гүйлгээний хүсэлт буруу байна.

6. ТХА-Н СИСТЕМИЙН ХАРИЛЦАН ХОЛБОЛТ

6.1. Худалдан авалтынQR үүсгэх (3051)

Тайлбар

Мерчантын терминал дээр төлбөр хүлээн авах QR код үүсгэх.

Хүсэлтийн өгөгдөл

Field	Mandatory	Description
srcInstId	M	Хүсэлт илгээсэн байгууллагын дугаар, МОСТ-с олгоно
channel	M	Гүйлгээний суваг
lang	M	Хэл
traceNo*	M	Хүсэлтийн трэйсийн дугаар
payeeId	M	Төлбөр хүлээн авагч мерчантын дугаар
posNo	M	Төлбөр хүлээн авагч терминалын дугаар
billId	O	Биллийн дугаар
tranAmount	M	QRтөлбөрийн дүн
tranCur	M	QR төлбөрийн валют
tranDesc	M	QR төлбөрийн гүйлгээний утга
deviceIP	O	Хүсэлт илгээсэн терминалын IP
deviceMac	O	Хүсэлт илгээсэн терминалын MAC
deviceName	O	Хүсэлт илгээсэн терминалын Name

Хүсэлтийн хариу

Field	Mandatory	Description
responseCode	M	Хүсэлтийн хариуны код
responseDesc	M	Хүсэлтийн хариуны тайлбар
traceNo	M	Хүсэлтийн трэйсийн дугаар
responseData	M	Хүсэлтийн хариуны утга /QR code image/

Жишээ

srcInstId, posNo, payeeId талбаруудыг Банк эсвэл МОСТ руу хандаж авна уу.

Request Header:

```
HttpWebRequest request =
(HttpWebRequest)WebRequest.Create("https://webpos.merchant.mn/ots/api/mapi/TT3
051");
byte[] data = System.Text.Encoding.UTF8.GetBytes(jsonBody);
request.Method = "POST";
request.ContentType = "application/json; charset=utf-8";
request.Accept = "application/json";
request.Headers.Add("Accept-Charset", "utf-8");
request.ContentLength = data.Length;
request.KeepAlive = false;
request.UseDefaultCredentials = true;

request.Headers.Add("PV", "03");
```

```
request.Headers.Add("TT", "3061");
request.Headers.Add("RS", "00");
```

Request Body:

```
{
  "srcInstId": "300000",
  "channel": "44",
  "lang": "0",
  "traceNo": "2017052405430504",
  "tranCur": "MNT",
  "tranAmount": "15000",
  "posNo": "1000",
  "payeeId": "1000",
  "tranDesc": "MAPI+"
}
```

Response:

```
{
    "responseCode": "0",
    "responseDesc": "",
    "traceNo": "2017052405430504",
    "responseData": "{
        "qr_code": "772966785344620171024141059585160160000000000070264",
        "qpay_account_id": "1215",
        "qr_image":
"iVBORw0KGgoAAAANSUhEUgAAASwAAAEsCAYAAAB5fY51AAAIBklEQVR42u3cwU0DURBEQYdCJgRF/
oIEOFrr7p560l7NeudP+WL8+pWkkl4egSRgSRKwJAFLkoAlScCSBCxJApYkAUsSsCQJWJIELEnAkiR
gSRKwJAFLkoAlScCSBKz/+/r5Pnul9a57TnudJ8+hvcjbC2ABC1jAApbBAAtY9gJYwAIWsIBlMMACF
rCAZTDAApa9ABawgAUsYBkMsIAFLGAZDLCAZS/KwGqscWlX7+fJRVqde/P5ARawgAUsYBkMsIBlL4A
FLGABC1jAAhawgAUsgwEWsOwFsIAFLGABC1jAAhawgGUwwAKWvRgEa/Xgri5J47xW4VvdC2ABC1jAA
pbBAAtY9gJYwAIWsIAFLGABC1jAMhhgActeAAtYwAIWsIAFLGABC1gGAyxgeV/AOgvW6k82N34w2At
gAQtYwLIXwAIWsIAFLIMBFrDsBbCABSxg2QtgAQtYwAKWwQALWPYCWMACFrCABSxgAQtYwDKYmUWCi
L0AlsEAy3O2F8ACFrCABSyDARZE7AWwDAZYnrO9ABawgAUsYBkMsCBiL4BlMMDyt+wFsIAFLGABK+Y
NPFHagUu758Z5reLYuBfAAhawgAUsgwEWsOwFsIAFLGABC1jAAhawgGUwwAKWvQAWsIAFLGABC1jAA
hawDAZYwLIXw2CtXo2IeJ2uD6rVvQAWsLwOsIBlMBbS6wALWMDyOsACFrCA5XWABSyDsZBeB1jAApb
XARawgAUsrwMsYBmMhfQ69qIULOUc3LR7blxs5QUsYAELWMASsIAlYAELWMACloAFLGABS8ACloAFL
GABC1gCFrCABSwBC1gClgX4MDQ+GPZmkXo2gAUsYAELWMACFrCABSxgAQtYwAIWsIAFLGABC1jAAha
wgAUsYAELWMACFrCABSxgAQtYQWCtfisaoJ2H+yIi6x9UwAIWsIAFLGABC1jAAhawgAUsYAELWMACF
rCABSxgAQtYwAIWsIAFLGABC1jAAhawgAWso2A5BF3QXAbU+QEWsCACLGABC1jAAhawgAUsYDk/wAI
WRIAFLGABC1jAAhawgAUs5wdYwIIIsIAFLGD5W8CaBMuAc3B88j8KLn94ND7n5h0EFrCABSxgAQtYw
AIWsIAFLGABC1jAAhawgAUsYAELWMACFrCABSxgAQtYwAIWsIAFLGAFgZW2kJcP0+WZrp7DxrMKLGA
BC1jAAhawgAUsYAELWC5gAQtYwAIWsIAFLGABC1jAApYLWMACFrCABSxgAQtYwDoOlsXe+wb/6vO5f
J5T7wdYwAKW8wwsYAELWMACFrCABSxgeaDAApbzDCxgAQtY7gdYwAIWsIDlgQILWIAAFrCABSz3EwR
W2oNo/Mb86v2A2LfzgQUIYAELWMACFrCABSxgAQtYwAIWIIAFLGABC1jAAhawgAUsYAELWIAAFrCAB
Sz3AyxgjYG1/vOsKYc77W+lfQitztT7AhawgAUsYAELWMACFrCABSxgAQtYwAIWsIAFLGABC1jAAha
wgAUsYAELWMACFrCABSxg1YG1+m1vy7YH1up79013YAELWMACFrCABSxgAQtYwAIWsIAFLGABC1jAA
hawgAUsYAELWMACFrCABSxgAQtYwAJW1IAdgq7S5t74odj4AeNfc4AFLGABC1jAAhawgAUsYAELWMA
CFrCABSxgAQtYwAIWsIAFLGABC1jAAhawgAUsYAHrOFiNi7R6uGG9d8ZWP4SABSxgAQtYDhOwgAUsY
```

```
AELWMACFrCABSxgActhAhawgAUsYAHLGQMWsIAFLGABy2ECFrCAdRysy4fAzyh3zd3PZ/umO7CABSx
nFVgOAbCABSxgAQtYwAIWsIAFLGcVWA4BsIAFLGABC1jAAhawgAUsZxVYDgGwgHUWrMs/TZu2AKuAp
p1DF7CABSxgAQtYwAKWC1jAAhawXMACFrCABSxgAQtYLmABC1jAcgELWMACFrCABSxguc6CpRyMGlF
b/Rb76gcMsIAFLGB5PsACFrCABSwBC1jAAhawgAUszwdYwAIWsIAlYAELWMACFrCA5fkAC1jAAtZxs
Hyj95kBN76v1b+1Onf/mgMsYAELWMACFrCABSxgAQtYwAIWsIAFLGABC1jAAhawgAUsYAELWMACFrC
ABSxgAQtYwKr7ZnDa+7IAfhp7ab+ABSxgAcv9AAtYwAIWsIAFLGABC1jAAhaw3A+wgAUsYAELWMACF
rCABSxgAcv9AAtYwAIEsM5+k/vJ95V2KEEMdGABC1jAAhawgAUsYAELWMACFrCABSxgAQtYwAIWsIA
FLGABC1jAAhawgAUsYAELWMACFrCA5RnGPsPGn3Vu/mljYAHLMwQWsCwbsIAFLGBZNs8QWMACFrA8Q
2ABy7IBC1jAApZl8wyBBSxgAcszBBawLBuwgAUsYFm2D/+tJ2eRluXvnDuwgAUsYAELWMACFrCABSw
HF1jAAhawgAUsYAELWMACFrCABSxgAQtYwAIWsIAFLGABC1iDYDUOD/o3sb4csAwGWMCyF8ACFrCcZ
2ABC1jAAhawgAUsYNkLYAELWMACFrCABSxgAQtYwAKWvQAWsIAFLGCdvdIOCoy6PhhW5w4sYAELWMA
CFrCABSxgAQtYwAIWsIAFLGABC1jAAhawgAUsYAELWMACFrCABSxgAQtYwBoGS5KAJUnAkgQsSQKWJ
GBJErAkCViSgCVJwJIkYEkCliQBS5KAJQlYkgQsSQKWJGBJErAkCViSxvoDDADZrnns3KQAAAAASUV
ORK5CYII="
    }"
}
```


6.2. Үүсгэсэн QR төлбөрийн хариу шалгах болон цуцлах хүсэлт (3065)

Тайлбар

Мерчантын терминал дээр үүсгэсэн QR кодыг төлөгдсөн эсэхийг сонсох хүсэлтийн цаг дууссан тохиолдолд төлбөр төлөгдсөн эсэхийг шалгуулах болон үүсгэсэн QR кодыг цуцлуулах хүсэлт явуулна.

Хүсэлтийн өгөгдөл

Field	Mandatory	Description
srcInstId	M	Хүсэлт илгээсэн байгууллагын дугаар, MOCT-с олгоно
channel	M	Гүйлгээний суваг
lang	M	Хэл
traceNo*	M	Хүсэлтийн трэйсийн дугаар
qrCode*	M	Төлбөрийн QR код
payeeId	M	Төлбөр хүлээн авагч мерчантын дугаар
posNo	M	Төлбөр хүлээн авагч терминалын дугаар
billId	M	Биллийн дугаар
isCheckQr	M	Төлбөр төлөгдсөн эсэхийг шалгах бол 1 цуцлах бол 0 гэж явуулна.
deviceIP	O	Хүсэлт илгээсэн терминалын IP
deviceMac	O	Хүсэлт илгээсэн терминалын MAC
deviceName	O	Хүсэлт илгээсэн терминалын нэр

Хүсэлтийн хариу

Field	Mandatory	Description
responseCode	M	Хүсэлтийн хариуны код
responseDesc	M	Хүсэлтийн хариуны тайлбар

traceNo	M	Хүсэлтийн трэйсийн дугаар
refNo	O	МОСТ дээрх гүйлгээний дугаар /isCheckQr = 1 үед/
tranDate	O	Гүйлгээний тайлант огноо /isCheckQr = 1 үед/
tranAmount	O	Гүйлгээний дүн /isCheckQr = 1 үед/
billId	O	Гадны нэхэмжлэхийн дугаар /isCheckQr = 1 үед/

6.3. ТАН-тай худалдан авалтын гүйлгээний хүсэлт (1608)

Тайлбар

ММ хэтэвчинд үүссэн ТАН кодыг ПОС дээр оруулж гүйлгээ дамжуулахад дараах параметрыг дамжуулна.

Хүсэлтийн өгөгдөл

Field	Mandatory	Description
srcInstId	M	Хүсэлт илгээсэн байгууллагын дугаар, МОСТ-с олгоно
channel	M	Гүйлгээний суваг
lang	M	Хэл
traceNo*	M	Хүсэлтийн трэйсийн дугаар
payeeId	M	Төлбөр хүлээн авагч мерчантын дугаар
posNo	M	Төлбөр хүлээн авагч терминалын дугаар
billId	O	Биллийн дугаар
srcMsisdn*	M	Худалдан авагчийн утасны дугаар
tan*	M	Худалдан авагчийн нэг удаагийн гүйлгээний нууц үг
tranAmount	M	Гүйлгээний дүн
tranCur	M	Гүйлгээний валют
tranDesc	O	Гүйлгээний утга
deviceIP	O	Хүсэлт илгээсэн терминалын IP
deviceMac	O	Хүсэлт илгээсэн терминалын MAC
deviceName	O	Хүсэлт илгээсэн терминалын нэр

Хүсэлтийн хариу

Field	Mandatory	Description
responseCode	M	Хүсэлтийн хариуны код
responseDesc	M	Хүсэлтийн хариуны тайлбар
traceNo	M	Хүсэлтийн трэйсийн дугаар
billId	O	Биллийн дугаар
refNo	O	МОСТ дээрх гүйлгээний дугаар
tranDate	O	Гүйлгээний тайлант огноо

tranAmount	O	Гүйлгээний дүн
feeAmount	O	Гүйлгээний шимтгэлийн дүн
vatUserNo	O	НӨАТУС-н хэрэглэгчийн дугаар

7. НУУЦЛАЛ

Гүйлгээний чухал талбаруудыг терминал дээрээс нууцалж дамжуулна. Энэ нууцалсан талбарууд ньдундаа задрахгүй явсаар МОСТ дээр ирж задрах ёстой.

Тэмдэглэгээнүүдийн тайлбар:

D – Нууцлах талбаруудыг агуулсан JSON форматтай текст /*-той талбарууд/
K – Нэг удаагийн түлхүүр. TraceNo эсвэл өөр давтагдашгүй утга байж болно.
SG – Signature
EK – Нууцлагдсан нэг удаагийн түлхүүр
SD – Нууцлагдсан мэдээлэл
PbKA – Мостын public key. Файл эсвэл текст утга байна.

Мерчантын ПОС–н терминалуудад МОСТ-ын PublicKey–г байрлуулна.

Мэдээллийг нууцлах алхамууд:

1. *SD = Encrypt1(D, K);*
2. *EK = Encrypt2(K, PbKA);*
3. *SG = Hash1(D);*

ГС –с нууцлалын алгоритмыг хэрэгжүүлсэн .NET жишээг оруулав.

```
string D = newJavaScriptSerializer().Serialize(secureData);
stringPbKA = "MostPublicKey";
stringK = traceNo;
ret.SD = Convert.ToBase64String(Encrypt1(Encoding.UTF8.GetBytes(D),
K));
ret.EK = Convert.ToBase64String(Encrypt2(Encoding.ASCII.GetBytes(K),
PbKA);
ret.SG = Convert.ToBase64String(Hash(Encoding.UTF8.GetBytes(D)));
```

Encrypt1 алгоритм:

AES128 битийн тэгш хэмт алгоритм ашиглана.
Cipher Mode нь CBC,
PaddingModeнь PKCS7.
IV нь:
{(byte)0xA1, (byte)0xE2, (byte)0xD5, (byte)0xFE, (byte)0xDA, (byte)0x52, (byte)0x0A, (byte)0x8F, (byte)0x8A, (byte)0x19, (byte)0xAA, (byte)0xBB, (byte)0x0A, (byte)0xD0, (byte)0x55, (byte)0xAC}
ГС –с нууцлалын алгоритмыг хэрэгжүүлсэн .NET жишээг оруулав.

```
staticbyte[] Encrypt1(byte[] data, string key)
```

```
{
	byte[] keyBytes = Encoding.UTF8.GetBytes(key);
	byte[] encBytes = null;
	using (MemoryStreamms = newMemoryStream())
	{
		byte[] ivBytes = { (byte)0xA1, (byte)0xE2, (byte)0xD5,
(byte)0xFE, (byte)0xDA, (byte)0x52, (byte)0x0A, (byte)0x8F, (byte)0x8A,
(byte)0x19, (byte)0xAA, (byte)0xBB, (byte)0x0A, (byte)0xD0, (byte)0x55,
(byte)0xAC };
		System.Security.Cryptography.AesCryptoServiceProvideraes =
newSystem.Security.Cryptography.AesCryptoServiceProvider();
		aes.Mode = CipherMode.CBC;
		aes.Padding = PaddingMode.PKCS7;
		ICryptoTransformencryptor = aes.CreateEncryptor(keyBytes,
ivBytes);
		CryptoStreamcryptoStream = newCryptoStream(ms, encryptor,
CryptoStreamMode.Write);
		cryptoStream.Write(data, 0, data.Length);
		cryptoStream.FlushFinalBlock();
		cryptoStream.Close();
		encBytes = ms.ToArray();
	}
	returnencBytes;
}
```

Encrypt2 алгоритм:

RSA тэгш бус хэмт алгоритм ашиглана.

OAEP (Optimal Asymatric Encryption Padding) хийхгүй..NET дээрх хэгжүүлсэн жишээ:

```
staticbyte[] Encrypt2(byte[] k, string key)
{
	RSACryptoServiceProviderrsa = newRSACryptoServiceProvider();
	rsa.FromXmlString(key);
	returnrsa.Encrypt(k, false);
}
```

Hash1:

SHA1 хаш байна..NET дээрх хэгжүүлсэн жишээ:

```
staticbyte[] Hash(byte[] data)
{
	SHA1CryptoServiceProvidersha = newSHA1CryptoServiceProvider();
	returnsha.ComputeHash(data);
}
```

8. СҮЛЖЭЭНИЙ ХОЛБОЛТ

Санхүүгийн байгууллага, гадны терминалтайхолболт тогтоох, сүлжээний холболт байгаа эсэхийг тусгай форматтай мессэжийг тодорхой давтамжтайгаар илгээж шалгаж байна.

8.1. Сүлжээний холболт шалгах хүсэлт

Field	Mandatory	Description
traceNo	M	Гүйлгээний трэйс дугаар
tranDate	O	Хүсэлт илгээсэн огноо

8.2. Сүлжээний холболт шалгах хүсэлтийн хариу

Field	Mandatory	Description
traceNo	M	Гүйлгээний трэйс дугаар
responseCode	M	Гүйлгээний хариу код

---------- ooo ----------