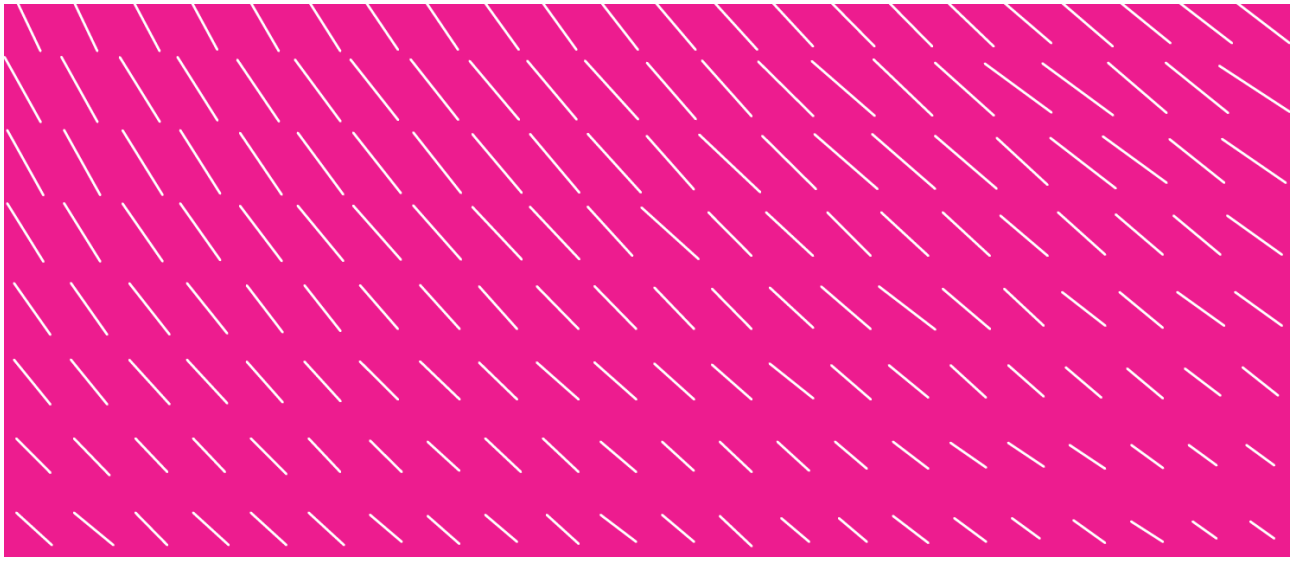


NET BANKING LINK

Secure link from online bank to external services

Service description and service provider's guidelines v 2.0

FINANCE FINLAND

Contents

Version history

1.3	26 May 2008	
2.0	29 Feb 2024	Updates to data security policy, text consistently brought up to date

Itämerenkatu 11–13
FI-00180 Helsinki
Finland
Tel: +358 20 793 4200
Fax: +358 20 793 4202
firstname.lastname@financefinland.fi
www.financefinland.fi
Twitter.com/finfinance

1 Net banking link description

The net banking link offers companies the opportunity to reduce the printing and distribution of paper documents. The link enables a consumer customer to move from the bank's online service to an external service provider's service while maintaining strong customer authentication.

The net banking link is governed by a standard jointly agreed by the banks. A non-bank service provider agrees on the implementation of the link with all the banks whose online banking customer are to be provided with the linked service.

1.1 General description

The net banking link is formed from an online banking transaction. It can be used to provide additional information or a more detailed itemisation of the transaction in an external service.

The link connects the online banking customer to the external service provider's display service on the Internet. The link contains all of the information the service provider needs to match the link with the right transaction.

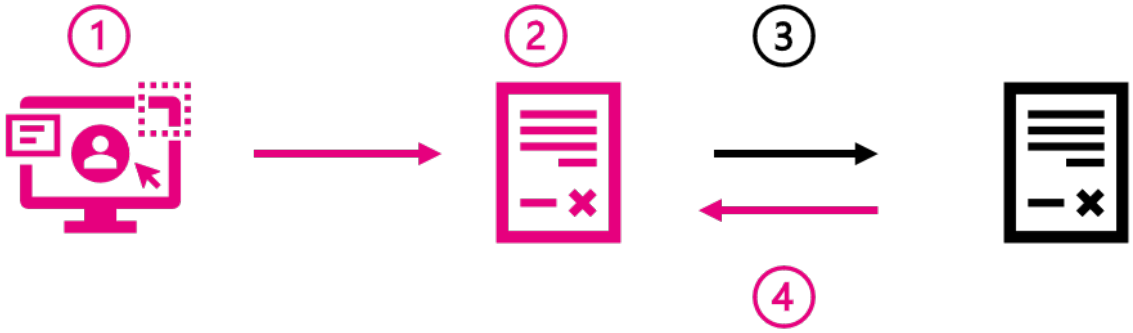
All transmitted data is encrypted, and the integrity of the data is secured with a message authentication code (MAC).

1.2 Application

The most typical use of the net banking link is in connection with consumer e-invoicing. The consumer wants to view more specific invoice information on an e-invoice they have received through the bank's online service. To do so, they will click the net banking link on the e-invoice to connect to the invoicing service provider's invoice display service.

Another common context in which the net banking link is used is when an online banking customer moves from the bank to an external e-salary service to view their own electronic payslip.

2 Functional description of the net banking link



This functional description illustrates the process through which a customer is routed to the e-invoice display service. The same logic applies with e-salary services.

1. The online banking customer logs into the bank's e-service (e.g. online bank or mobile application) and opens an incoming e-invoice.

2. The e-invoice in question includes a net banking link.

3. The link connects the customer to the service provider's online display service. The invoice information can be displayed in a new browser tab or window, for example.

4. When the customer leaves the service provider's service (e.g. by closing the browser tab), they are taken back to the bank's online service and can then authorise the payment of the invoice, for example.

If the online banking service times out while the customer is on the external service provider's website, the customer must log back into the online bank.

3 Implementation of the net banking link

The service provider agrees on the implementation of the link separately with each bank. The starting date of the service is agreed in the contract. The service provider's contract data is registered at each bank, and it must notify each bank separately if there are changes to the data.

Once the service contract is signed, the bank provides the service provider with the service identifier and MAC key used in the service. The information is delivered to the service provider either electronically or in paper format, depending on the bank's own policy. During physical transfer, the information must be secured in a way that enables the recipient to detect if it has been breached (e.g. with a tamper-evident envelope).

The link testing procedures are bank-specific, and more information about them is available in the banks' own service descriptions.

4 Security

The communications between the online bank and the display service are protected with the Transport Layer Security (TLS) protocol, which prevents third parties from viewing or altering any data. The service provider's data in the service that the net banking link points to must also be protected with the TLS protocol. The TLS protocol version must be at least as recent as 1.2.

Each bank authenticates its online banking customers. The information forwarded from the bank to the display service via the net banking link is based on the invoice details and the details of the online banking customer. The integrity of the information carried in the link is secured with an message authentication code (MAC), which prevents the online banking customer from altering the information

5 Parameters of the net banking link

The net banking link character string consists of the values of the parameter fields, with an ampersand (&) separating the fields. The name of the field and the value are connected using the equals sign (=) character. The character string ends with the message authentication code followed by an ampersand (&).The character string may not contain whitespace characters.

All character strings use ISO 8859-1 encoding unless otherwise specified.

URL	Length	Description
https://www.yritys.fi/aaaa/bbbbbb/cccccccc	max 2,048 characters	• protocol, TLS encryption • server name • name of the display service on the server

Field name	Value	Length	Description
VERSION	0001 or 0020 0020 = version 2.0 (updated in 2024)	4 numbers	Version number of the link
PMTREFNB		max 96 characters	Unique identifier of the transaction which the link targets. • in e-salary services, the wage recipient's Finnish personal identity code (e.g. 123456-789X) in encrypted format • max length of plaintext representation of the encrypted data is 64 characters • max length of encrypted representation of the encrypted data is 96 characters • in consumer e-invoices (Finvoice), max length 60 characters

			• archiving identifier of any additional data related to the invoice (e.g. creditor reference, which the invoicer enters in the field InvoiceUrlText in a Finvoice e-invoice) • PMTREFNB is not encrypted in consumer e-invoices If the value in PMTREFNB is encrypted, the link's message authentication code (MAC) is calculated from the encrypted value. For a more detailed description of the encryption of the parameter, see section 5.2.
RCVID		max 20 characters	The invoicer's or paymaster's identifier at the bank. Not used in consumer e-invoices.
TIMESTMP	YYYY-MM-DD-HHMMSS+HH or YYYY-MM-DDHHMMSS%2BHH	22 or 24 characters	Link generation date and time. Time zone is displayed as +HH or %2BHH depending on the bank. +02 = %2B02 = standard time in Finland +03 = %2B03 = daylight saving time in Finland. For a more detailed description of the use of the parameter, see section 5.1.
KEYVERS	0000..9999	4 numbers	Version of the MAC key. Value range 0000–9999. For a more detailed description of the use of the parameter, see section 5.4.
ALG	0003 = SHA-256 0004 = SHA-512	4 numbers	MAC key calculation algorithm.
LANGCODE	1 = Finnish 2 = Swedish 3 = English	1 number	Customer's language code in the online banking service.
SESSIONID		max 20 characters	Unique session identifier assigned by the bank. Logged for potential later use in e.g. auditing or troubleshooting the transaction.
SENDID		max 20 characters	Unique identifier of the party that generates the link. In a consumer e-invoice, the SENDID value is the BIC of the bank which generated the link.
MAC			The link's message authentication code (MAC), i.e. a checksum calculated from all of the link

			parameters. The checksum is calculated by the server that generates the link. The MAC is represented in upper-case hexadecimal in the MAC parameter field. If the MAC of a link does not match the checksum calculated from the link parameters, the link is rejected.
STATUS	Prod = production link Test = testing link	4 characters	Status of the link.
Optional parameters			
PMTORIG	1 = consumer e-invoice 2 = e-salary	1 number	Payment input method.
ENCALG	0001 = AES-256-CBC	4 numbers	Encryption algorithm.
ENCKEYVER	0000..9999	4 numbers	Version of the encryption key. Value range 0000–9999. For more information on the use of the parameter, see section 5.5.
USERMAC		32 characters	Checksum calculated from the payer's personal identity code. For a more detailed description of the use of the parameter, see section 5.3.

5.1 Detailed description of the use of TIMESTMP

The receiving service must verify that the link was not used more than 15 minutes before or 15 minutes after the timestamp was generated. This is verified by comparing the values of the TIMESTMP and PMTREFNB parameters. A single net banking link can only be used once.

5.2 Detailed description of the encryption of PMTREFNB

The PMTREFNB field is encrypted using the Advanced Encryption Standard's (AES) cipher block chaining mode (CBC), which has a 16-byte (128 bits) initialisation vector (IV). The IV parameter must not be predictable: it must be generated randomly or pseudo-randomly, and the same IV must never be reused. This notwithstanding, it is not necessary to retain a log of all used IV parameters if the pseudorandom number generator that was used does not have any known vulnerabilities. The number of possible IV parameter values is so large that the likelihood of accidental clashes of identical values can be considered negligible.

The length of the cipher key is 256 bits.

The plaintext data that is to be encrypted must use the character set ISO 8859-1. The standard size of a plaintext block is 16 characters (bytes). If necessary, the plaintext

can be padded with whitespace characters. It may not contain the ampersand (&) or equals sign (=) character.

The resulting ciphertext begins with a 16-byte IV parameter; the same length as a standard AES block. This is immediately followed by the actual 16-byte ciphertext (one 16-byte AES block). The total length of a cipher block is thus 32 bytes. The entire cipher block – IV and ciphertext included – is represented in hexadecimal with the letters A to F in upper case. The length of this hexadecimal representation is 64 characters.

If the PMTREFNB field is encrypted, the link's message authentication code (MAC) is calculated using the hexadecimal representation of the encrypted value.

5.2.1 Example calculation of an encrypted value in PMTREFNB field

The plaintext block starts with the information that is to be encrypted, which in this case is a personal identity code (010101-999X). The rest of the block is padded with whitespaces.

The plaintext input:

```
”010101-999X      ”
```

The full plaintext block in hexadecimal:

```
30313031303130312D393939582020202020
```

The IV in hexadecimal:

```
1457A63E941796F59DE04108938402A8
```

The binary value of the key in hexadecimal:

```
62C12760C2E68990DDD45FB77442161AAC39D454DB5A6454BAB599ACCE56C522
```

The encrypted PMTREFNB field value in hexadecimal:

```
1457A63E941796F59DE04108938402A8C335092F6D378CF934114772AF4DC905
```

5.3 Detailed description of the use of USERMAC

In some situations, the display service may need to verify whether the user of the online banking service is the same as the user authorised to view specific information or perform specific actions.

The verification is done from the encrypted personal identity code in the USERMAC parameter.

USERMAC is calculated in the same way as the full link's MAC (see sections 5.6.1 and 5.7.1) as follows:

- The time stamp, personal identity code and MAC key are concatenated together, separated with the '&' character (TIMESTMP&IDENTITYCODE&KEY&)
- The personal identity code includes the separator character. The separator character and the control character are in upper case if they are letters.
- A hash value for the character string is calculated using the algorithm defined in ALG. The hash value is stored in the USERMAC field in upper-case hexadecimal.

If the display service has a log of authorised persons which includes their personal identity codes, the match can be verified by building the same character string from the invoicer's information, calculating a message authentication code for the string, and comparing the resulting checksum with the value of the USERMAC field.

Note: This method requires that the personal identity codes are recorded in the display service provider's system, because they are not carried in plaintext on the net banking link.

If the encryption key used to calculate the USERMAC key is known, the USERMAC parameter should not be treated as a sufficient means to secure the user's personal identity code. This must be taken into account when the data security of the net banking link is evaluated.

5.4 Detailed description of the use of KEYVERS

The KEYVERS parameter stores the version number of the encryption key used to calculate the MAC and USERMAC checksums. The version number value can range between 0000 and 9999. The value increases sequentially with time, with the oldest version having the smallest version number.

If there is any reason to suspect that a third party has gained access to the key, it must be updated to a newer version. Both parties (display service provider and bank) are obligated to request a key change if there is the slightest suspicion it has been compromised.

After the first time that the display service is accessed through a valid link using the new key, the display service must reject all requests that use an older key but have a more recent TIMESTMP than the first link to use the new key version. Such requests are always unauthorised and malicious and indicate that the older key has been compromised.

Correspondingly, once a new key version has been taken into use, the bank must no longer generate net banking links using a MAC or USERMAC that has been signed with the older key. The only exception can be made if it has become clear that the newer version links do not work in the display service. Under normal circumstances, the bank must not, without pressing reason, switch to the new key until it has been taken into use in the display service.

Once the parties have exchanged the new encryption key, the old key must expire within 24 hours. From the moment of expiration, the display service must reject all

links that use the old key version, and the bank must not generate new net banking links in which the MAC or USERMAC has been signed with the expired key version.

5.5 Detailed description of the use of ENCKEYVER

The ENCKEYVER parameter stores the version number of the encryption key used to encrypt PMTREFNB. The version number value ranges between 0000 and 9999. The value increases sequentially, with the oldest version having the smallest version number.

If there is any reason to suspect that a third party has gained access to the key, it must be updated to a newer version. Both parties are obligated to request a key change if there is the slightest suspicion it has been compromised.

Once the parties have exchanged the new encryption key, the old key must expire within 24 hours. From the time of expiration, all links generated using the old key must be rejected by the display service. and the bank must not generate new net banking links which contain data signed using the expired key version.

5.6 Consumer e-invoice link

The link is generated in the online banking service according to bank-specific rules from an e-invoice that the customer opens for viewing.

The link parameters enable the link to be pointed to the correct invoice in the invoice display service.

Regarding the link parameters, note the following:

- SENDID is the bank's BIC
- PMTREFNB stores the archiving identifier of additional data related to the consumer e-invoice (e.g. creditor reference, which the invoicer enters in field InvoiceUrlText in a Finvoice invoice)
- RCVID is not used

Before the link is approved, its parameter fields and values must be validated against the following rules. If all of the conditions are not met, the link must be rejected.

1. The link must include all of the mandatory parameters listed below.
2. Each mandatory parameter must occur only once.
3. Each optional parameter can occur only once.
4. The link must not include any other parameters besides the mandatory and optional parameters listed below.
5. Each parameter must only include the specified characters.
6. Each parameter must only include the specified number of characters.
7. A parameter value must not include the ampersand (&) or equals sign (=) character.

Mandatory link parameters:

- VERSION
- PMTREFNB

- TIMESTMP
- KEYVERS
- ALG
- LANGCODE
- SESSIONID
- SENDID
- STATUS
- MAC

Optional link parameters:

- PMTORIG
- ENCALG
- ENCKEYVER
- USERMAC

Example:

```
https://www.yritys.fi/aaaa/bbbbbb/cccccccc?VERSION=0020&PMT
REFNB=12345678901 234567890&TIMESTMP=2021-11-16-
102030%2B02&KEYVERS=0001&ALG=0003&LANGCODE=1&SESSIONID=1234
5&STATUS=Prod&SENDID=NDEAFIHH&PMTORIG=1&ENCALG=0001&ENCKEYV
ER=0001&USERMAC=12345678901234567890123456789012&MAC=A62B3A
510736BE134CA0CADC8EB06F051455E93E81C7A617CE4B878C2B2E6626
```

5.6.1 Calculation of MAC for a consumer e-invoice

The character string from which the message authentication code (MAC) is calculated consists of the values of the parameter fields, with an ampersand (&) separating the fields. Example:

```
VERSION&PMTREFNB&TIMESTMP&KEYVERS&ALG&LANGCODE&SESSIONID&ST
ATUS&SENDID&PMTORIG&ENCALG&ENCKEYVER&USERMAC&
```

The parameters are concatenated together always in the same order. If an optional parameter is not included in the link, its position in the string is filled with an empty, zero-length value.

The character string ends with the MAC key followed by an ampersand (&).The character string may not contain whitespace characters. This gives us:

```
VERSION&PMTREFNB&TIMESTMP&KEYVERS&ALG&LANGCODE&SESSIONID&ST
ATUS&SENDID&PMTORIG&ENCALG&ENCKEYVER&USERMAC&MAC&
```

If URL encoding has been used, it must be decoded from the parameters before calculating the MAC.

A hash value is calculated for the character string using the algorithm defined in ALG. The hash value is stored in the USERMAC field in upper-case hexadecimal.

Note: If the MAC value contains lower-case characters, they are first converted into upper case.

Example:

```
https://www.yritys.fi/aaaa/bbbbbb/cccccccc?VERSION=0020&PMT
REFNB=12345678901234567890&TIMESTMP=2021-11-16-
102030%2B02&KEYVERS=0001&ALG=0003&LANGCODE=1&SESSIONID=1234
5&STATUS=Prod&SENDID=NDEAFIHH&PMTORIG=1&ENCALG=0001&ENCKEYV
ER=0001&USERMAC=12345678901234567890123456789012&MAC=A62B3A
510736BE134CA0CADC8EB06F051455E93E81C7A617CE4B878C2B2E6626
```

The binary value of the MAC key used in the above example in hexadecimal:

```
A3DD23F6611F9185B9A00A6ADF1DEC023775DD0B860AE902971C2D06E1E
4F7DC
```

The entire character string from which the example's hash value is calculated:

```
0020&12345678901234567890&2021-11-16-
102030+02&0001&0003&1&12345&Prod&NDEAFIHH&1&0001&0001&12345
67890123456789012345678901 2&A3DD23F6611F9185B9A00A6ADF1DEC0
23775DD0B860AE902971C2D06E1E4F7DC&
```

Note: The URL-encoded %2B in the TIMESTMP value is decoded into a plus sign (+) before calculation: 2021-11-16-102030%2B02 is thus 2021-11-16-102030+02 in the calculation.

The entire character string from which the example's hash value is calculated, represented in hexadecimal:

```
303032302631323334353637383930313233343536373839302632303232
12D31312D31362D3130323033302B3032263030303126303030332631263
13132333435265072 6F64264E4445414649484826312630303031263030303
031263132333435363738393031323334353637383930313233343536373
838930313226413344443233463636313146393138354239413030413641
444631444543303233373735444430423836304145393032393731433244
430364531453446374443 26
```

Hash value:

```
A62B3A510736BE134CA0CADC8EB06F051455E93E81C7A617CE4B878C2B2
E6626
```

5.7 Link generated in the online banking service

This section discusses the link which takes the user to an external e-salary service, for example.

Before the link is approved, its parameter fields and values must be validated against the following rules. If all of the conditions are not met, the link must be rejected.

1. The link must include all of the mandatory parameters listed below.
2. Each mandatory parameter must occur only once.
3. Each optional parameter can occur only once.
4. The link must not include any other parameters besides the mandatory and optional parameters listed below.
5. Each parameter must only include the specified characters.
6. Each parameter must only include the specified number of characters.
7. A parameter value must not include the ampersand (&) or equals sign (=) character.

Mandatory link parameters:

- VERSION
- PMTREFNB
- RCVID
- TIMESTMP
- KEYVERS
- ALG
- LANGCODE
- SESSIONID
- SENDID
- STATUS
- MAC

Optional link parameters:

- PMTORIG
- ENCALG
- ENCKEYVER
- USERMAC

Example:

```
https://www.yritys.fi/aaaa/bbbbbb/cccccccc?VERSION=0020&PMT
REFNB=3DF281BAA8B82D28AFB8E7AD531C36835280DC3EC965065B8A4BE
E651E4199AB6FE14BD2D3BFF3931CEF96B0C2D6115C&RCVID=12345678&
TIMESTMP=2021-11-16-102030+02&KEYVERS=0001&ALG=0004&MAC=
FD34904641D3728B7699F4C8208DE8E1EF25A49B726902C81F59572D30B
1A9681C9FE7443BCC21F7B6F8FE58F88BF618A62F246FE415FF50F4EF84
039CDBD439&LANGCODE=1&SESSIONID=1234567890123456789O&SENDID
=PLACEHOLDER&STATUS=Prod&PMTORIG=1&USERMAC=1234567890123456
7890123456789012&ENCALG=0001&ENCKEYVER=0001
```

5.7.1 Calculation of the net banking link's MAC

The character string from which the message authentication code (MAC) is calculated consists of the values of the parameter fields, with an ampersand (&) separating the fields. Example:

```
VERSION&PMTREFNB&RCVID&TIMESTMP&KEYVERS&ALG&LANGCODE&SESSIO
NID&STATUS&SENDID&PMTORIG&ENCALG&ENCKEYVER&USERMAC&
```

The parameters are concatenated together always in the same order. If an optional parameter is not included in the link, its position in the string is filled with an empty, zero-length value.

The character string ends with the MAC key followed by an ampersand (&).The character string may not contain whitespace characters. This gives us:

```
VERSION&PMTREFNB&RCVID&TIMESTMP&KEYVERS&ALG&LANGCODE&SESSIO
NID&STATUS&SENDID&PMTORIG&ENCALG&ENCKEYVER&USERMAC&MAC&
```

If URL encoding has been used, it must be decoded from the parameters before calculating the MAC.

A hash value is calculated for the character string using the algorithm defined in ALG. The hash value is stored in the USERMAC field in upper-case hexadecimal.

Note: If the MAC value contains lower-case characters, they are first converted into upper case.

Example:

```
https://www.yritys.fi/aaaa/bbbbbb/cccccccc?VERSION=0020&PMT
REFNB=3DF281BAA8B82D28AFB8E7AD531C36835280DC3EC965065B8A4BE
E651E4199AB6FE14BD2D3BFF3931CEF96B0C2D6115C&RCVID=12345678&
TIMESTMP=2021-11-16-102030+02&KEYVERS=0001&ALG=0004&MAC=
FD34904641D3728B7699F4C8208DE8E1EF25A49B726902C81F59572D30B
1A9681C9FE7443BCC21F7B6F8FE58F88BF618A62F246FE415FF50F4EF84
039CDBD439&LANGCODE=1&SESSIONID=1234567890123456789O&SENDID
=PLACEHOLDER&STATUS=Prod&PMTORIG=1&USERMAC=1234567890123456
7890123456789012&ENCALG=0001&ENCKEYVER=0001
```

The binary value of the MAC key used in the above example in hexadecimal:

```
A3DD23F6611F9185B9A00A6ADF1DEC023775DD0B860AE902971C2D06E1E
4F7DC
```

The entire character string from which the example's hash value is calculated:

```
0020&3DF281BAA8B82D28AFB8E7AD531C36835280DC3EC965065B8A4BEE
651E4199AB6FE14BD2D3BFF3931CEF96B0C2D6115C&12345678&2021-
11-16-102030+02&0001&0004&1&1234567890123456789O&Prod&
PLACEHOLDER&1&0001&0001&12345678901234567890123456789012&A3
DD23F6611F9185B9A00A6ADF1DEC023775DD0B860AE902971C2D06E1E4F
7DC&
```

Note: The URL-encoded %2B in the TIMESTMP value is decoded into a plus sign (+) before calculation: 2021-11-16-102030%2B02 is thus 2021-11-16-102030+02 in the calculation.

The entire character string from which the example's hash value is calculated, represented in hexadecimal:

```
3030323026334446323831424141384238324432384146423845374144
3
5333143333638333532383044433345433936353036354238413442454
5
3635314534313939414236464531344244324433424646333933314345
4
6393642304332443631313543263132333435363738263230323120313
1
2D31362D3130323033302B3032263030303126303030342631263132333
4
3536373839303132333435363738393026507265426504C414345484F
4C4445522631263030303126303030312631323334353637383930313233
3435363738393031323334353637383930313226413344443233463636
3131463931383542394130304136414446314445433032333737354444
3
0423836304145393032393731433244303645314534463744432
6
```

Hash value:

```
FD34904641D3728B7699F4C8208DE8E1EF25A49B726902C81F59572D30B
1A9681C9FE7443BCC21F7B6F8FE58F88BF618A62F246FE415FF50F4EF84
039CDBD439
```