Aktia Identification Service

Instructions for use and record description

30th September 2016, version 1.4

Table of contents

1. Aktia Identification Service

The Aktia Identification Service helps service providers to reliably identify their online customers using the bank's identification methods. In the Aktia Identification Service, the bank identifies the customer on behalf of the service provider. The Aktia Identification Service is available 24/7, excluding breaks due to maintenance, updates, etc.

The Aktia Identification Service is based on the TUPAS standard drawn up by the Finnish Bankers' Association and it is aimed at providers of electronic business and payment services. The identification data transferred in the Aktia Identification Service may be used as part of the formation of an electronic signature if the customer to be identified and the service provider have so agreed.

More information about the standard is available on the Federation of Finnish Financial Services website www.fkl.fi.

2. General

The customer to be identified is key to the use of the service. The customer directs the transfer of his or her information between the service provider and the bank. The bank and the service provider are not in direct contact with each other during the service.

The identifier generated is unique and tied to the service provider's service event and the customer in question. When a service provider has a need to identify a customer, the service provider sends an identifier request to the customer, who will enter the Identification Service by clicking on Aktia's identification button. The service provider's identification request is relayed to the bank's Identification Service, which sends a response to the customer after identification. The customer checks the information he or she has received and accepts it, after which he or she returns to the service provider's service and continues there activities related to that service. If the customer so wishes, he or she can cancel or reject the identification event, either before identification or after checking the response message, in which case the customer's information will not be transferred to the service provider.

The possibility to use service information as part of an electronic signature is based on an agreement between the service provider and the customer on the possibility to use identification information as part of an electronic signature in a legal transaction between them. The use of the Aktia Identification Service as an electronic signature is further supported by timestamps and log data of response messages. However, if the service is to be used as a part of signing an agreement or making an application, the service provider must ensure that other issues required by electronic signatures have been seen to, including management of data as a whole, saving of the response message and the invariability of the service. Aktia shall not be liable for the validity or content of any agreement or any other legal action between the service provider and the customer to be identified.

The address of the online service is https://auth.aktia.fi/tupas
Aktia Identification Service is available 24/7.

2.1 Agreements

The service provider shall enter into a written agreement with the bank on the use of the Aktia Identification Service. The service provider's information will be registered at the bank and the contact person referred to in the agreement will be sent the second part of the Checksum Key in a safe manner to be agreed separately. The first part of the Checksum Key will be printed on the agreement.

Aktia Identification Service has supported version 0003.

The bank will enter into an agreement on transferring the social security number only when the service provider has the right to register it.

The length of the checksum key used in the service and the service provider's right to register social security numbers shall be included in the agreement.

The service provider must inform a branch of the bank of any changes to their service or information. When needed, the branch will revise the agreement with the changed information.

2.2 Name and logo of Aktia Identification Service

The names ‘Aktia tunnistus’ or ‘Aktia identifiering’ may be used for the bank's online identification service. Other names may not be used. The logo of ‘Aktia tunnistus’ is the trademark of Aktia Bank.

The company providing the service shall copy the logo to their own server from Aktia's server at http://www.aktia.fi/fi/verkkomaksu-tunnistuspalvelu-logo.fi. The size and colours of the logo may not be changed.

The logo/name may not be transferred or used for any other purpose than those agreed in the Aktia Identification Service agreement.

After the agreement has terminated, the service provider must, without delay, delete the Aktia Identification Service's logo/name from its website.

3. Security

The SSL encryption protocol is used in data communications between the Identification Service parties to ensure that the information cannot be seen or modified by outsiders. The service provider's server software must support 256-bit SSL encryption. However, the key length used with the connection will be determined on the basis of the features of the browser used by the customer. Information related to the identification request and response message are protected with a checksum ensuring the integrity of the information, so the customer directing the transfer of identification information does not have a possibility to change the information without the service provider and Aktia Identification Service being aware of it.

Each party shall be liable for securing their own services and the accuracy of the information stored by them.

The users of the service shall be liable for ensuring that their online banking IDs are not disclosed to outsiders and that the access codes are given only to the computer

used for the Aktia Identification Service. The user of the service shall also check the service provider from the identification information returned by the Aktia Identification Service and accept the transfer of Aktia identification.

3.1 Changing and storing the checksum key

The checksum key will be valid for two years starting from the first successful detection event it is used. The second part of the checksum key will be sent to the customer when the key in use has 60 days of validity left.

The checksum key will be delivered to the contact person referred to in the agreement. At the same time, the contact person will receive information about the version number of the new key as well as the date when it enters into force. The checksums will be counted with the key in question starting from said date.

In order to ensure flexible change of keys, the service provider's system must enable a new key to be entered in advance, i.e. the simultaneous use of two checksum keys. At the time of the change, for approximately 15 minutes, it is possible that some of the checksums received by the service providers are calculated with the old key while some are calculated with the new key.

When the new checksum key has been successfully used, the old key may be removed or its use blocked in the service provider's system.

The service provider must store the MAC checksum key carefully and keep it safe from unauthorised use.

4. Functional description

The Aktia Identification Service has numerous features and use possibilities depending on what has been agreed about the nature of the response message in the service agreement. Identification information of the response message always contains the name of the customer. In addition, the identification information transferred may be either in plaintext or encrypted.

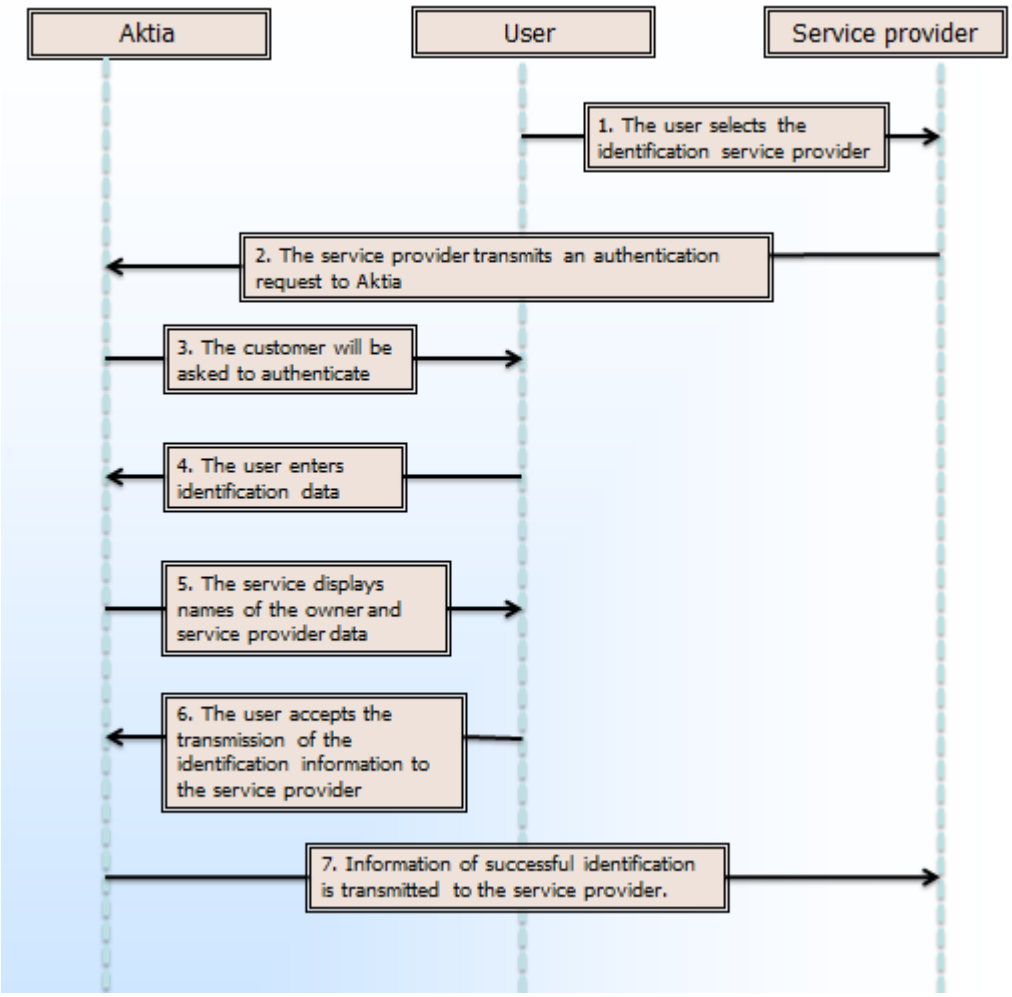
When the response message is in plaintext, Aktia will transfer either the customer's social security number, the specifying part of the social security number or a business ID according to what has been agreed in the service agreement. The Aktia Identification Service will transfer social security numbers in plaintext to service providers with the right to process them.

When the identification information is encrypted, the Aktia Identification Service will transfer a checksum based on the customer's social security number or business ID to the service provider. However, the number itself will not be transferred with the response message. The service provider must have the customer's social security number or business ID at their use to verify the accurate verification of the information received in the response message given by the Aktia Identification Service. If the service provider does not possess the customer's ID, they must ask for it before the identification request is sent. Consequently, this functionality is suited for checking the information given by the customer from the bank.

Functionalities utilising the customer's social security number are suited, for example, to the identification of the customer, logging in the service and making binding

agreements. The specifying part of the social security number may be used, for example, for logging in to a service after registration to the service.

4.1 Service progress



Graph key

1. The user to be identified is in contact with the service provider's service.
2. The service provider has a need to identify service users. The identification request includes the information required by the Identification Service about the service provider and the identification event. Aktia will check the integrity of the request, the accuracy of the information and the service provider's Identification Service agreement.
3. Aktia will give the user an identification request if the request from the service provider is error-free. Aktia will give the user an error message if errors are detected in the identification request. If they so wish, users can interrupt identification and return to the service provider's service.
4. The users identify themselves using Aktia's online banking IDs. An error message will be displayed to the user if identification fails.
5. The user checks the identification information. Aktia recognises the service provider on the basis of their customer ID and displays the name of the registered service provider to the user.

6. The user accepts the transfer of the identifier to the service provider. If they so wish, the user can reject the identifier by clicking the "cancel" button and return to the service provider's service.
7. Aktia will notify the service provider about successful identification enhanced with the user's identification information agreed with the service provider and ends the user's session in the service provided by Aktia.

5. Message descriptions of Aktia Identification Service

5.1 Identifier request

Identification request information is behind the Aktia identification icon in FORM information group as a latent variable.

FORM INFORMATION GROUP				
Field	Name of information	Length	Obligation	Note
1. Message type	A01Y_ACTION_ID	3–4	P	Standard, "701"
2. Version	A01Y_VERS	4	P	0003
3. Service provider	A01Y_RCVID	10–15	P	Service ID
4. Service language	A01Y_LANGCODE	2	P	FI = Finnish SV = Swedish
5. Individualisation of the query	A01Y_STAMP	20	P	Vvvvkkpphhmmssxxxxxx
6. Identifier type	A01Y_IDTYPE	2	P	01 = Encrypted basic ID 02 = Basic ID in plaintext 03 = Shortened basic ID in plaintext
7. Return address	A01Y_RETLINK	199	P	OK return address for identifier
8. Cancel address	A01Y_CANLINK	199	P	Return address when cancelling
9. Rejected address	A01Y_REJLINK	199	P	Return address in an error situation
10. Key version	A01Y_KEYVERS	4	P	The key's generation information
11. Algorithm	A01Y_ALG	2	P	03 = SHA256
12. Checksum	A01Y_MAC	64	P	Query checksum key

The names of the information fields are written in capital letters. The structure of the FORM information group in HTML is as follows:

```
<FORM METHOD=“POST” ACTION=“https://auth.aktia.fi/tupas”>
<INPUT NAME= “A01Y_ACTION_ID” TYPE=“hidden” VALUE=“701”>
<INPUT NAME= “A01Y_VERS” TYPE=“hidden” VALUE=“...”>
<INPUT NAME=“A01Y_RCVID” TYPE=“hidden” VALUE=“...”>
<INPUT NAME=“A01Y_LANGCODE” TYPE=“hidden” VALUE=“...”>
<INPUT NAME=“A01Y_STAMP” TYPE=“hidden” VALUE=“...”>
<INPUT NAME=“A01Y_IDTYPE” TYPE=“hidden” VALUE=“...”>
<INPUT NAME=“A01Y_RETLINK” TYPE=“hidden” VALUE=“...”>
<INPUT NAME=“A01Y_CANLINK” TYPE=“hidden” VALUE=“...”>
<INPUT NAME=“A01Y_REJLINK” TYPE=“hidden” VALUE=“...”>
<INPUT NAME=“A01Y_KEYVERS” TYPE=“hidden” VALUE=“...”>
<INPUT NAME=“A01Y_ALG” TYPE=“hidden” VALUE=“...”>
<INPUT NAME=“A01Y_MAC” TYPE=“hidden” VALUE=“...”>
</FORM>
```

5.2 Key to the identification request fields

1. Message type, which is standard 701.

2. Version number of identification request message, which is 0003 (ISO-8859-1).

3. Service provider's customer ID. The Aktia Identification Service identifies the service provider based on their customer ID and links the service provider's name in its register with the name's identification message. The ID has been marked in the section “Service ID” and “Checksum” in the agreement form drawn up with the bank. The ID is a character string without any punctuation marks. For example, the service ID may be 1234567890 and the checksum 123, making the service provider's ID 1234567890123.

4. The service language code indicates the language of the service provider's service page and the Aktia Identification Service will open with this language if the language in question is among the current language selection of Aktia tunnistus.

5. An individualising ID given to the identification request by the service provider. The ID may be a reference, customer number or a combination of date, time, running ID and reference number.

6. The identifier type indicates which individualisation information the service providers wants for the customer to be identified. The identifier type must correspond with the functionality agreed in the service agreement.

   i. 01 = Encrypted basic ID A hexadecimal-format MAC checksum calculated on the basis of the customer's identifier information, May include the customer's social security number or business ID in full.

   ii. 02 = Basic ID in plaintext May include the customer's social security number or business ID in full.

   iii. 03 = Shortened basic ID in plaintext May include the specifier part of the social security number without the character indicating the century or the business ID in its entirety.

7. The address of the service provider's service page, which is the continuation point in an OK case. The return address has to begin with ‘https’, i.e. it has to be SSL-encrypted.

   i. Example: VALUE=https://www.verkkokauppa.fi/tilaus/vahvistus.html

8. The continuation point of the service provider's service, if the customer cancels the transfer of the identifier.

   i. Example: VALUE=https://www.verkkokauppa.fi/tilaus/keskeytys.html

9. The continuation point of the service provider's service, if a technical error has been detected in identification.

   i. Example: VALUE=https://www.verkkokauppa.fi/tilaus/virhe.html

10. Key version used in the calculation of the MAC checksum.

11. The algorithm type code used in the calculation of the MAC checksum. Aktia identifier uses 03 = SHA-256 algorithm, which produces a 64-character MAC.

12. MAC identifier, which has been calculated from the data to be secured in the identification request and the service provider's checksum key with the algorithm defined in information field 11. The recipient uses the checksum to verify the integrity and the sender of the identification request

5.3 Generation of the MAC checksum of the identification request

The service provider will generate an identification request for the bank's function button, which will be secured with a MAC checksum. The checksum is calculated from the FORM information group of the identification request with a checksum key given to the service provider by the Aktia Identification Service.

The calculation starts with a string of VALUE numbers in the FORM information group of all information fields (fields 1–11) preceding the checksum and the service provider's checksum key. The information will be combined as a string so that the blanks used for filling the fields will be discarded. The information groups in the string are separated by an ampersand ("&"). An ampersand ("&") will be placed between the last piece of information (field 12) and the checksum key as well as at the end of the checksum key. Ampersands ("&") will be included in the calculation of the MAC checksum. Information is given in one row. A plus sign ("+") indicates a line break in the document.

A01Y_ACTION_ID&A01Y_VERS&A01Y_RCVID&A01Y_LANGCODE&A01Y_STAMP&+
A01Y_IDTYPE&A01Y_RETLINK&A01Y_CANLINK&A01Y_REJLINK&A01Y_KEYVERS&+
A01Y_ALG&checksumkey&

The calculated MAC will be changed to a hexadecimal format where A–F is represented with capital letters. The value of the hexadecimal version will be exported to the MAC checksum field.

5.4 Response message and identifier

The Aktia Identification Service will add response message information in the "OK" return link in query-string format.

The checksum will be calculated from the original message after which Scandinavian characters and certain special characters (such as whitespace, equals signs and inverted commas) will be replaced with the equivalent hexadecimal sign (for example, “%20”) in the data communications message.

The Aktia Identification Service will calculate the MAC checksum of the response message with a service provider-specific key. The checksum allows the service provider to ensure that the identifier has been generated at the customer's bank and that the identifier message information has not changed.

RESPONSE MESSAGE				
Field	Name of information	Length	Obligation	Note
1. Version	B02K_VERS	4	P	0003
2. Individualisation of the identifier	B02K_TIMESTMP	23	P	NNNvvvvkkpphhmmssxxxxxx
3. Number of the identifier	B02K_IDNBR	10	P	Number generated for the identifier by the Aktia Identification Service
4. Individualisation of	B02K_STAMP	20	P	Query information field 7

the query				(A01Y_STAMP)
5. Customer	B02K_CUSTNAME	40	P	Customer's name
6. Key version	B02K_KEYVERS	4	P	Generation of the key
7. Algorithm	B02K_ALG	2	P	03 = SHA256
8. Identifier	B02K_CUSTID	40	P	Encrypted checksum or plaintext service ID
9. ID type	B02K_CUSTTYPE	2	P	00 = not known 01 = social security number in plaintext 02 = social security number specifier in plaintext 03 = business ID in plaintext 04 = electronic service user ID in plaintext 05 = encrypted social security number 06 = encrypted business ID 07 = encrypted electronic service user ID
10. Checksum	B02K_MAC	AN 64	P	Checksum key of the response

5.5 Key to the response message fields

1. Version number of response message, which is 0003 (ISO-8859-1).

2. A timestamp generated by the bank's system, where NNN is always 410 and indicates that the system in question is the Aktia Identification Service.

3. Information given to the identifier by the bank's information system, which individualises the identifier in the bank's system.

4. Identification request individualisation information, which has been retrieved from information field 7 of the identification request in question (A01Y_STAMP)

5. Name of the customer from the bank's customer database.

6. MAC checksum key generation information.

7. The MAC algorithm ID.

8. The customer's identifier information. ID in plaintext or encrypted identifier depending on the content of the A01Y_IDTYPE field of the identification request.

9. Identifier type. This field indicates what the identifier information in field 8 is. Possible values are:
   01 = social security number in plaintext
   02 = social security number specifier in plaintext
   03 = business ID in plaintext
   04 = electronic service user ID in plaintext Not used in the Aktia Identification Service.
   05 = protected social security number
   06 = protected business ID
   04 = encrypted electronic service user ID. Not used in the Aktia Identification Service.

10. Response message checksum.

5.6 Calculation of the response message checksum

The integrity of the received response message will be checked by first calculating a checksum for it, which will be compared with the checksum of the message. The checksum will be calculated from information fields 1–9 of the response messages. The content of the B02K_CUSTID field is determined based on what ID was requested in the identification request and, consequently, it is either an encrypted checksum or a customer ID in plaintext.

When checksum is calculated you should bear in mind that encoding of the response message is ISO-8859-1 (in version 0003). If encoding changes during the processing the checksum might not match. When calculating the checksum the information and the checksum key will be separated by an ampersand ("&"), which will also be added to the end of the checksum key. A service provider-specific key is used in checksum calculation. A plus sign ("+") indicates a line break in the document.

B02K_VERS&B02K_TIMESTMP&B02K_IDNBR&B02K_STAMP&+
B02K_CUSTNAME&B02K_KEYVERS&B02K_ALG&+
B02K_CUSTID&B02K_CUSTTYPE&checksumkey&

5.7 Identifier type

The type of customer identifier to be transferred affects the checksum calculation, which is determined in the A01Y_IDTYPE field of the identification request. The customer identifier is either: (1) customer ID in plaintext, or (2) encrypted checksum.

1. Customer ID in plaintext as customer identifier

The values of the A01Y_IDTYPE field “02” and “03”: Basic ID in plaintext or a shortened basic ID.

The customer ID is either a string of characters in plaintext, for example, a social security number or its end in accordance with the A01Y_IDTYPE field of the identification request. The identifier will be paced as it is as information in the response message B02K_CUSTID.

2. Encrypted identifier as customer ID

The value of the A01Y_IDTYPE field is “01”, i.e. an encrypted basic ID.

The bank uses the same algorithm for encrypting the customer ID which is used in checksum calculation of messages. The identifier information is encrypted using the information from message information fields 2–4 in the response and the customer's ID registered at the bank (social security number or a business ID). When calculating the encrypted ID, the information and the checksum key will be separated by an ampersand (“&”), which will also be added to the end of the checksum key. A service provider-specific key is used in encryption. A plus sign ("+") indicates a line break in the document.

B02K_TIMESTMP&B02K_IDNBR&B02K_STAMP&+
customerID&checksumkey&

The calculated ID will be changed into a hexadecimal format where the values A–F are represented with capital letters. The end result is a string, which is placed in the response message as information B02K_CUSTID.

5.8 Checking the message checksum and identification of the customer

The service provider will calculate the MAC checksum of the message received in a manner described in section 5.6. If it is the same as the checksum in the response message from the bank, the response message has been transferred unchanged.

If an encrypted ID has been used in the response message, the service provider will check the accuracy of the customer ID in its use from the response message's information fields and the ID in its use in the manner described in section 5.7. If the checksum received corresponds to the content of the identifier field of the response message (B02K_CUSTID), the service provider has the correct customer identifier in their use.

6. Exceptional situations

The service provider must prepare for exceptional situations which may include:

1. The customer interrupts the identification event. The customer may interrupt an event either before the transfer of the identifier to the Aktia Identification Service or after the creation of the identifier by clicking the “Cancel” button, the address of which is the Cancel address in FORM information field 8 of the identifier request.

2. Verification of a customer may fail due to inaccuracy of identification information provided by the customer or because the customer has asked for identification from the wrong bank.

3. The Aktia identification Service detects an error in the identifier request message.

4. The service provider detects an error in the response message, which may be due to an error in the content of the message or the identifier not corresponding to the information given by the customer. The service provider must display a notice corresponding to the situation to the customer.

5. There is no response at all. The cause of the interruption may be a connection failure or other technical failure or the customer has left the session incomplete.

6. The same response appears several times. The service provider must prepare for the customer sending the same response several times or for the customer sending an old response message when moving from one window of the browser to the next using the “forward” and “back” buttons.

7. Implementation of the Aktia Identification Service

7.1 Preconditions

The service provider's system must be capable of generating an identification request using web technology. When the user has approved the transfer of the identifier to the service provider, the identifier must be linked with the assignment given by the user and stored as long as the assignment. Identifiers may not be entered into a register or used for any other purpose.

The Aktia Identification Service does not require any specific web server software but the software must support 256-bit SSL encryption.

7.2 Testing

The service implementation date will be settled in conjunction with the signing of the agreement.

Service providers have the opportunity to test the service in the production environment before an agreement is signed by using test IDs.

The address of the online service's test version: https://auth.aktia.fi/tupastest.

Service agreements used in test versions

Service provider (A0IY_RCVID)	Customer's name	Checksum key (secret key)	Type of agreement (A01Y_IDTYPE)
2222222222222	Testiyritys Oy	1234567890123456789012345678901234567890123456789012345678901234	Encrypted basic ID (01)
3333333333333	Testiyritys Oy	1234567890123456789012345678901234567890123456789012345678901234	Basic ID in plaintext (02)
4444444444444	Test organisation	1234567890123456789012345678901234567890123456789012345678901234	Shortened ID in plaintext (03)

The key version in all is 0001.

Customer IDs used in the test version

Customer's ID	Customer's name	Social security number	Password	Security number
12345678	Tero Testi Äyrämö	010170-999R	123456	1234

Example of message fields

IDENTIFIER REQUEST TEST MESSAGE Form information field	
A01Y_ACTION_ID	701
A01Y_VERS	0003
A0IY_RCVID	2222222222222
A01Y_LANGCODE	see description
A01Y_STAMP	see description
A01Y_IDTYPE	see description
A01Y_RETLINK	see description
A01Y_CANLINK	see description
A01Y_REJLINK	see description
A01Y_KEYVERS	0001
A01Y_ALG	03
A01Y_MAC	see description

RESPONSE MESSAGE	
B01Y_VERS	0003
B02K_TIMESTMP	see description
B02K_IDNBR	see description
B01Y_STAMP	Query information field A01Y_STAMP
B02K_CUSTNAM	Äyrämö Testi Tero
B01Y_KEYVERS	0001
B01Y_ALG	03
B02K_CUSTID	Basic number: 010170-999R Shortened number: 999R Encrypted number: Calculated from number 010170-999R
B02K_CUSTTYPE	see description
B01Y_MAC	see description

Checksum calculation example

IDENTIFIER REQUEST TEST MESSAGE Form information field	
A01Y_ACTION_ID	701
A01Y_VERS	0003
A0IY_RCVID	2222222222222
A01Y_LANGCODE	fi
A01Y_STAMP	2342392232323
A01Y_IDTYPE	01
A01Y_RETLINK	https://www.esimerkki.fi/tupasreturn
A01Y_CANLINK	https://www.esimerkki.fi/tupascancel
A01Y_REJLINK	https://www.esimerkki.fi/tupasreject
A01Y_KEYVERS	0001
A01Y_ALG	03
A01Y_MAC	53818C40A8637B4D744DC3E7A7C23FCD0C6F3E6F2F672E B403B3A04284A7E1B8

The checksum is calculated from the character string.

701&0003&2222222222222&fi&2342392232323&01&https://www.esimerkki.fi/tupasreturn&https://www.esimerkki.fi/tupascancel&https://www.esimerkki.fi/tupasreject&0001&03&1234567890123456789012345678901234567890123456789012345678901234&

After MAC calculation and hexadecimal conversion, the checksum is:
53818C40A8637B4D744DC3E7A7C23FCD0C6F3E6F2F672EB403B3A04284A7E1B8

8. Guidance and technical support

Customer connection guidance from Aktia Customer Service,tel. +358 10 247 6700 or E-mail: yritys@aktia.fi. More information regarding service time and telephone fees via address www.aktia.fi.

Appendix

The service uses the 8-bit ISO 8859-1 (Latin 1) character set, the codes of which are listed in the table attached.

æ	%00	0	%30	`	%60	‘	%90	À	%c0	ð	%f0
	%01	1	%31	a	%61	’	%91	Á	%c1	ñ	%f1
	%02	2	%32	b	%62	“	%92	Â	%c2	ò	%f2
	%03	3	%33	c	%63	”	%93	Ã	%c3	ó	%f3
	%04	4	%34	d	%64	•	%94	Ä	%c4	ô	%f4
	%05	5	%35	e	%65	–	%95	Å	%c5	õ	%f5
	%06	6	%36	f	%66	—	%96	Æ	%c6	ö	%f6
	%07	7	%37	g	%67		%97	Ç	%c7	÷	%f7
Backspace	%08	8	%38	h	%68	˜	%98	È	%c8	ø	%f8
Tab	%09	9	%39	i	%69	™	%99	É	%c9	ù	%f9
Linefeed	%0a	:	%3a	j	%6a	š	%9a	Ê	%ca	ú	%fa
	%0b	;	%3b	k	%6b	›	%9b	Ë	%cb	û	%fb
	%0c	<	%3c	l	%6c	oe	%9c	Ì	%cc	ü	%fc
C return	%0d	=	%3d	m	%6d		%9d	Í	%cd	ý	%fd
	%0e	>	%3e	n	%6e		%9e	Î	%ce	þ	%fe
	%0f	?	%3f	o	%6f	Ÿ	%9f	Ï	%cf	ÿ	%ff
	%10	@	%40	p	%70		%a0	Ð	%d0		
	%11	A	%41	q	%71	¡	%a1	Ñ	%d1		
	%12	B	%42	r	%72	¢	%a2	Ò	%d2		
	%13	C	%43	s	%73	£	%a3	Ó	%d3		
	%14	D	%44	t	%74		%a4	Ô	%d4		
	%15	E	%45	u	%75	¥	%a5	Õ	%d5		
	%16	F	%46	v	%76	|	%a6	Ö	%d6		
	%17	G	%47	w	%77	§	%a7		%d7		
	%18	H	%48	x	%78	¨	%a8	Ø	%d8		
	%19	I	%49	y	%79	©	%a9	Ù	%d9		
	%1a	J	%4a	z	%7a	ª	%aa	Ú	%da		
	%1b	K	%4b	{	%7b	«	%ab	Û	%db		
	%1c	L	%4c	|	%7c	¬	%ac	Ü	%dc		
	%1d	M	%4d	}	%7d	¯	%ad	Ý	%dd		
	%1e	N	%4e	~	%7e	®	%ae	Þ	%de		
	%1f	O	%4f		%7f	¯	%af	ß	%df		
Space	%20	P	%50	€	%80	°	%b0	à	%e0		
!	%21	Q	%51		%81	±	%b1	á	%e1		
”	%22	R	%52	‚	%82	²	%b2	â	%e2		
#	%23	S	%53	ƒ	%83	³	%b3	ã	%e3		
$	%24	T	%54	„	%84	´	%b4	ä	%e4		
%	%25	U	%55	…	%85	µ	%b5	å	%e5		
&	%26	V	%56	†	%86	¶	%b6	æ	%e6		
’	%27	W	%57	‡	%87	·	%b7	ç	%e7		
(	%28	X	%58	ˆ	%88	¸	%b8	È	%e8		
)	%29	Y	%59	‰	%89	¹	%b9	É	%e9		
*	%2a	Z	%5a	Š	%8a	º	%ba	Ê	%ea		
+	%2b	[	%5b	‹	%8b	»	%bb	Ë	%eb		
,	%2c	\	%5c	OE	%8c	¼	%bc	Ì	%ec		
-	%2d	]	%5d		%8d	½	%bd	Í	%ed		
.	%2e	^	%5e	Ž	%8e	¾	%be	Î	%ee		
/	%2f	_	%5f		%8f	¿	%bf	ï	%ef		