Session Layer - Logon

This topic describes the secure CME Globex logon process and scenarios for iLink and Drop Copy including:

CME Globex API Secure Logon

CME Globex requires secure authentication for iLink and Drop Copy sessions on Convenience Gateway (CGW) and Market Segment Gateway (MSGW).

The logon procedure secures the client system logon with:

- **Customer identity verification** - a client system logon request will be *signed* with security credentials issued and validated by CME Group.

- **Message confidentiality and integrity** - to credential the logon message, the client system sends a keyed-hash message authentication code (HMAC) generated from a combination of the logon FIX tag values. When CME Globex receives the logon message, it uses the identical inputs to calculate the HMAC value to validate against the logon request. If the values do not match, CME Globex rejects the logon.

> iLink and Drop Copy customers must use the logon procedure for all CME Group markets, including Partner Exchange markets hosted on the CME Globex platform.

> Customers must create secure key pairs for iLink and Drop Copy Sessions in the CME Customer Center.

> For more information on HMAC, please refer to:
>
> - Hash-Based Message Authentication
> - HMAC Examples
> - HMAC Cryptography

Testing and Certification

Certification via AutoCert+ is required for the CME Globex API secure logon. An iLink and Drop Copy certification suite is currently available in AutoCert+.

Note: Customers must create secure key pairs for New Release and CERT iLink and Drop Copy Sessions in the Request Center NR/CERT.

Click here to access the help file to learn about the Request Center NR/CERT.

Please contact your Global Account Manager if you do not have access to create secure key pairs for iLink and Drop Copy Sessions.

iLink and Drop Copy Security Credentials

When the client system submits a secure Logon message to iLink or Drop Copy, the message will contain the security credentials required for identity and permissions verification.

For both CGW and MSGW iLink sessions, to best support route-through sessions:

- Security credentials are validated at the Session ID level (the left-most 3 characters of tag 49-SenderCompID).
- For **iLink route-throughs**, the credentials assigned to the Session ID can be used by all SenderCompIDs associated with that session.

Security credentials are secure key pairs available only to the customer and the CME Globex platform.

- Access Key ID – used to sign Logon request to iLink or Drop Copy
- Secret Key – used to create HMAC signature

Secure Key Pair Creation and Management in the CME Customer Center

When a customer creates a secure key pair, the credentials can be viewed and downloaded in the CME Customer Center.

- Once created, credentials are accessible and available for multiple downloads in the CME Customer Center.
    - Clients are limited to 10 2FA tokens for logon and download per day.
- A customer can have up to two secure key pairs for a Session ID for up to four weeks, after which the older secure key pair is automatically expired.
    - A newly created secure key pair will have a status of *active,* i.e. valid for logon.
    - The first secure key pair will expire in four weeks after the market close.
- If a customer generates a third secure key pair:
    - One of the existing secure key pairs will be deleted, effective immediately, based on the customer selection.
    - The remaining secure key pair will expire in four weeks after the market close.

> ⚠ The Request Center is closed on weekends, from 4:30 pm Friday to 10:00 am Sunday CT.

For security reasons, CME Group requires customers to change their security credentials every 12 months. Notification regarding pending security credential expiration will be sent to registered administrators.

> ⚠ In a Disaster Recovery (DR) scenario, if a customer has created or managed the secure key pair (Access Key ID + Secret Key) in production within 15 minutes prior to the disaster event, that security credential change may not be reflected in the DR environment; in such an unlikely event, customers should generate a new secure key pair upon CME Globex transition to the DR environment.

Logon Procedure

This section describes the steps to sign a logon request to iLink and Drop Copy. These steps are:

1. Create Canonical FIX Message.
2. Create Signature using Secret Key provided by CME and Canonical FIX Message
3. Populate Algorithm ID plus Access Key ID plus HMAC Signature in the credentials fields of the logon message

Step 1 - Create Canonical FIX Message

To sign a logon request to iLink and Drop Copy, create a string that includes the following information from the logon FIX tag values. All values used to create the signature must match exactly to the tag values in the Logon message.

FIX tag values must be assembled in this order and values concatenated into a single string delimited by the new line character (i.e. '\n').

> ⚠ Only the tag value—not the tag number—must be used for the calculation of HMAC signature.
>
> Example: where tag 34=<999>, use only '999'.

- tag 34-MsgSeqNum – sequence number sent by client system
- tag 49-SenderCompID – sender comp ID including the Fault Tolerance Indicator (right-most character)
- tag 50-SenderSubID – Operator ID
- tag 52-SendingTime – timestamp in milliseconds, UTC time format. UTC Timestamps are sent in number of nanoseconds since Unix epoch synced to a master clock to microsecond accuracy.
- tag 57-TargetSubID – recipient of message.
    - For iLink and Drop Copy sessions,
        - CGW session – 'G'
        - MSGW session - two digit market segment ID
- tag 108-HeartBeatInterval – heartbeat interval specified in the logon message as number of seconds
- tag 142-SenderLocationID – assigned value used to identify specific message originator's location (i.e. geographic location)
- tag 369-LastMsgSeqNumProcessed – last message sequence number processed by the client system
    - This is an optional tag.
- tag 1603-ApplicationSystemName – identifies system generating the message
- tag 1604-ApplicationSystemVersion – identifies the version of the system generating the message
- tag 1605-ApplicationSystemVendor – identifies the vendor of the application system

Example of creating canonical FIX message

Step 2 - Create Signature using Secret Key and Canonical FIX Message

The signature is a Base64 URL Encoding of the Canonical Message created in Step 1 using the Secret Key provided by CME.

> ⓘ The Secret Key downloaded from Request Center is **Base64 URL Encoded**. Customers must decode the secret key first before using it.

In pseudo code:

Base64 URL Encoding (HmacSHA256(CanonicalFIXMessage, SecretKey));

Example Signature: oHZ2Dx1ihFAp7kHOFcJPkijm27xfApJFp-ZhsSCxr3s

Example of creating Base 64 URL Encoding using HMAC SHA256

Signature calculation in Java:

```
public String calculateHMAC(String canonicalRequest, String userKey) {
    String hash = null;

    try {
        // Init HMAC instance
        Mac sha256HMAC;
        sha256HMAC = Mac.getInstance("HmacSHA256");

        // Initialize HMAC instance with the key
        // Decode the key first, since it is base64url encoded
        SecretKeySpec secretKey = new SecretKeySpec(Base64.getUrlDecoder().decode(userKey), "HmacSHA256");
        sha256HMAC.init(secretKey);

        // Calculate HMAC, base64url encode the result and strip padding
        hash = Base64.getUrlEncoder().withoutPadding().encodeToString((sha256HMAC.doFinal(canonicalRequest.
getBytes("UTF-8"))));

    } catch (NoSuchAlgorithmException | InvalidKeyException | IllegalStateException |
UnsupportedEncodingException e) {
        e.printStackTrace();
    }

    return hash;
}
```

Signature calculation in C++:

```
// This exmaple is using Crypto++ library version 5.6.5 from https://www.cryptopp.com/
// g++ -I/usr/include/cryptopp hmacexample.cpp -o hmac.exe -lcryptopp -lpthread
#include <iostream>
using std::cout;
using std::cerr;
using std::endl;

#include <string>
using std::string;

#include <cstdlib>
using std::exit;

#include "cryptopp/cryptlib.h"
using CryptoPP::Exception;

#include "cryptopp/hmac.h"
using CryptoPP::HMAC;

#include "cryptopp/sha.h"
using CryptoPP::SHA256;
```

```
#include "cryptopp/base64.h"
using CryptoPP::Base64URLEncoder;
using CryptoPP::Base64URLDecoder;

#include "cryptopp/filters.h"
using CryptoPP::StringSink;
using CryptoPP::StringSource;
using CryptoPP::HashFilter;

string calculateHMAC(string &key, string &canonicalRequest)
{

    string decoded_key, calculatedHmac, encodedHmac;

    try
    {
        // Decode the key since it is base64url encoded
        StringSource(key, true,
            new Base64URLDecoder(
                new StringSink(decoded_key)
            ) // Base64URLDecoder
        ); // StringSource

        // Calculate HMAC
        HMAC < SHA256 > hmac((byte*)decoded_key.c_str(), decoded_key.size());

        StringSource(canonicalRequest, true,
            new HashFilter(hmac,
                new StringSink(calculatedHmac)
            ) // HashFilter
        ); // StringSource
    }
    catch(const CryptoPP::Exception& e)
    {
        cerr << e.what() << endl;
        exit(1);
    }

    // base64url encode the HMAC and strip padding
    StringSource(calculatedHmac, true,
        new Base64URLEncoder(
            new StringSink(encodedHmac)
        ) // Base64URLEncoder
    ); // StringSource


    return encodedHmac;
}
```

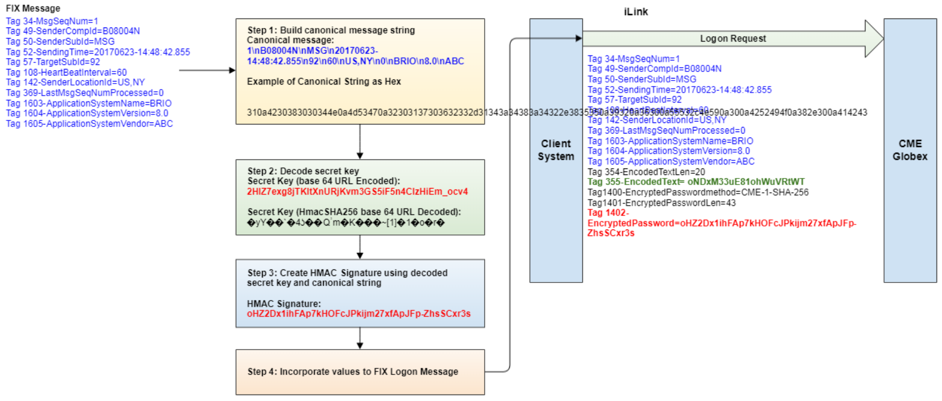
Step 3 - Populate Algorithm ID plus Access Key ID plus HMAC Signature in the new credentials fields of the logon message

- tag 354-EncodedTextLen - contains the length of AccessKeyID
- tag 355-EncodedText - contains the AccessKeyID
- tag 1400-EncryptedPasswordMethod - contains the AlgorithmID defined as CME-1-SHA-256
- tag 1401-EncryptedPasswordLen - contains the length of the HMAC signature
- tag 1402-EncryptedPassword - contains the HMAC signature. HMAC signature must be encoded in Base 64 Encoding with URL and Filename Safe Alphabet.

If any of these tags are missing, the client systems will receive a Logout message in response. The Logout message will not include detailed rationale for the failure to help protect the security of client sessions.

Secure Logon from Client System to CME Globex

This diagram illustrates the data processing required for the client system to submit a secure Logon message to CME Globex.


FIX Message
Tag 34-MsgSeqNum=1
Tag 49-SenderCompId=B08004N
Tag 50-SenderSubId=MSG
Tag 52-SendingTime=20170623-14:48:42.855
Tag 57-TargetSubId=92
Tag 108-HeartBeatInterval=60
Tag 142-SenderLocationId=US,NY
Tag 369-LastMsgSeqNumProcessed=0
Tag 1603-ApplicationSystemName=BRIO
Tag 1604-ApplicationSystemVersion=8.0
Tag 1605-ApplicationSystemVendor=ABC
Step 1: Build canonical message string
Canonical message:
1\nB08004N\nMSG\n20170623-14:48:42.855\n92\n60\nUS,NY\n0\nBRIO\n8.0\nABC
Example of Canonical String as Hex
310a4230383030344e0a4d53470a32303137303632332d31343a34383a34322e3835350a39320a36300a55532c4e590a300a4252494f0a382e300a414243
Step 2: Decode secret key
Secret Key (base 64 URL Encoded):
2HIZ7exg8jTKItXnURjKvm3GS5iF5n4ClzHiEm_ocv4
Secret Key (HmacSHA256 base 64 URL Decoded):
�yY��`�4J��Q'm�K���~[1]�1�o�r�
Step 3: Create HMAC Signature using decoded secret key and canonical string
HMAC Signature:
oHZ2Dx1ihFAp7kHOFcJPkijm27xfApJFp-ZhsSCxr3s
Step 4: Incorporate values to FIX Logon Message
iLink
Logon Request
Client System
CME Globex
Tag 34-MsgSeqNum=1
Tag 49-SenderCompId=B08004N
Tag 50-SenderSubId=MSG
Tag 52-SendingTime=20170623-14:48:42.855
Tag 57-TargetSubId=92
Tag 108-HeartBeatInterval=60
Tag 142-SenderLocationId=US,NY
Tag 369-LastMsgSeqNumProcessed=0
Tag 1603-ApplicationSystemName=BRIO
Tag 1604-ApplicationSystemVersion=8.0
Tag 1605-ApplicationSystemVendor=ABC
Tag 354-EncodedTextLen=20
Tag 355-EncodedText= oNDxM33uE81ohWuVRtWT
Tag1400-EncryptedPasswordmethod=CME-1-SHA-256
Tag1401-EncryptedPasswordLen=43
Tag 1402-EncryptedPassword=oHZ2Dx1ihFAp7kHOFcJPkijm27xfApJFp-ZhsSCxr3s

When CME Globex receives the logon request, it performs the same steps as the client system did to calculate the HMAC signature as follows:

1. Confirm the access key is accurate and assigned to the logon message's Session ID expected.
2. Compare the timestamp (tag 52-SendingTime) in the client Logon message (tag 35-MsgTpe=A) with the current time. To ensure the timestamp value submitted in tag 52 is current, CME Group strongly recommends following Network Time Protocol guidleines.
    - A timestamp older than *5* seconds will be rejected as stale.
3. Calculate and compare HMAC signature to that on Logon request.

    - If the HMAC signatures match, the logon message is authentic and validates that the sender has the secret key.
        - CME Globex will send a Logon (tag 35-MsgType=A) response to client system.
    - If the HMAC signatures do not match, the logon request is rejected.
        - CME Globex will send a Logout **(tag 35-MsgType=5)** message to the client system.

    Error conditions could apply to these scenarios:

    - Logon message is missing any of the new security credentials fields
        - 58=Invalid Logon. All Required Fields are not Present. Missing Tag <number>. Logout Forced
    - Logon message contains invalid Algorithm ID
        - 58=Invalid Logon. Invalid EncryptedPasswordMethod(tag 1400). Logout Forced
    - Logon message contains HMAC signature which cannot be decoded using Base 64 Encoding with URL and Filename Safe Alphabet
        - 58=Invalid Logon. Logout Forced
    - Logon message is missing all the new security credentials fields
        - 58=Invalid Logon. Logout Force
    - Logon message is pending HMAC validation and another logon attempt is made (not in-session)
        - 58=Invalid Logon. Logon Already in Progress. Logout Forced
    - HMAC authentication times out

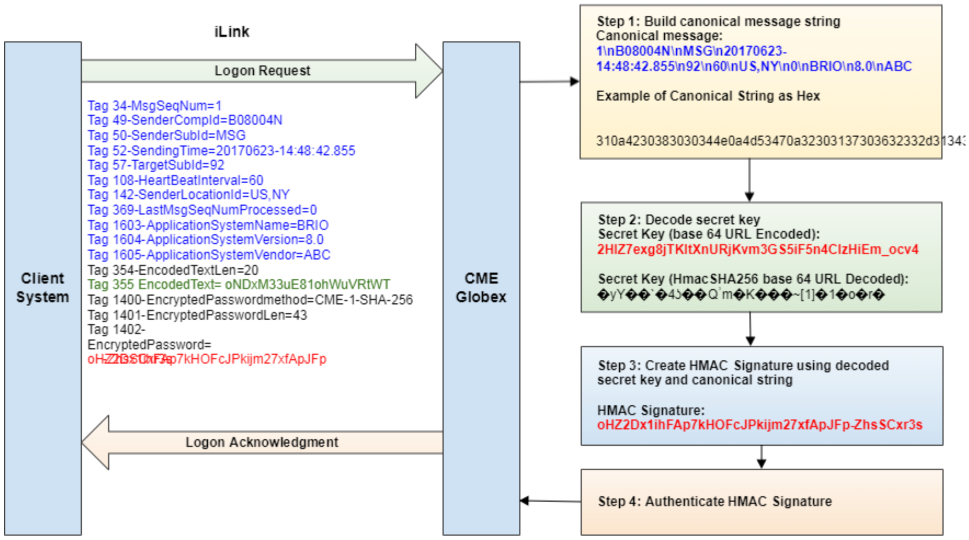
        - 58=Logon Could not be Authenticated at This Time. Please Try Again Later. Logout Forced

    - HMAC authentication response contains incorrect SenderCompID
        - 58=Invalid Logon. Logout Forced
    - HMAC authentication response fails because HMAC Signature does not match
        - 58=Invalid Logon. Logout Forced
    - HMAC authentication response fails because Access Key ID does not match
        - 58=Invalid Logon. Logout Forced

⚠ Invalid Logon (tag 35=**A**) due to HMAC authentication will be counted towards Automated iLink Port Closure.

Secure Logon from CME Globex to Client System

This diagram illustrates how CME Globex validates the secure client Logon using the same inputs used by the client system to generate the HMAC signature.


iLink
Logon Request
Tag 34-MsgSeqNum=1
Tag 49-SenderCompId=B08004N
Tag 50-SenderSubId=MSG
Tag 52-SendingTime=20170623-14:48:42.855
Tag 57-TargetSubId=92
Tag 108-HeartBeatInterval=60
Tag 142-SenderLocationId=US,NY
Tag 369-LastMsgSeqNumProcessed=0
Tag 1603-ApplicationSystemName=BRIO
Tag 1604-ApplicationSystemVersion=8.0
Tag 1605-ApplicationSystemVendor=ABC
Tag 354-EncodedTextLen=20
Tag 355 EncodedText= oNDxM33uE81ohWuVRtWT
Tag 1400-EncryptedPasswordmethod=CME-1-SHA-256
Tag 1401-EncryptedPasswordLen=43
Tag 1402-
EncryptedPassword=
oHZ2Dx1ihFAp7kHOFcJPkijm27xfApJFp
Logon Acknowledgment
Client System
CME Globex
Step 1: Build canonical message string
Canonical message:
1\nB08004N\nMSG\n20170623-14:48:42.855\n92\n60\nUS,NY\n0\nBRIO\n8.0\nABC
Example of Canonical String as Hex
310a4230383030344e0a4d53470a32303137303632332d31343
Step 2: Decode secret key
Secret Key (base 64 URL Encoded):
2HIZ7exg8jTKltXnURjKvm3GS5iF5n4ClzHiEm_ocv4
Secret Key (HmacSHA256 base 64 URL Decoded):
�yY��`�4Ͻ��Q˚m�K���~[1]�1�o�r�
Step 3: Create HMAC Signature using decoded secret key and canonical string
HMAC Signature:
oHZ2Dx1ihFAp7kHOFcJPkijm27xfApJFp-ZhsSCxr3s
Step 4: Authenticate HMAC Signature

Tag 52-SendingTime Validation

iLink and Drop Copy logon requests must reach CME Globex within 5 seconds to prevent a stale logon. Timestamps (tag 52-SendingTime) submitted by the client system in the Logon (tag 35-MsgTpe=A) message older than 5 seconds will be rejected. CME Globex will send a Logout (tag 35-MsgType=5) message to the client system.

> ⓘ To ensure the timestamp value submitted in tag 52 is current, CME Group strongly recommends the following Network Time Protocol guidelines.

Logon Scenarios

Client systems use the Logon (tag 35-MsgType=A) message for authentication with CME Globex. There are three Logon scenarios:

- **Beginning of Week Logon** – the very first logon message the client system sends for the week. Client systems **must set** their inbound and outbound sequence numbers to '**1**' prior to the Beginning of Week Logon for a successful logon.
- **Mid-Week Logon** – used for any subsequent logons, after the beginning of the week. Following mid-week log off, the client system logs in mid-week with the next sequential outbound message sequence number.
- **In-Session Logon** – used to reset sequence numbers while the client system is already logged on.

> ⓘ If there is a logon failure, the client system must reset the inbound and outbound sequence number to '1' until the client system establishes a successful Beginning of Week Logon.

> ⚠ The client system must submit the Logon message within 60 seconds after establishing a TCP/IP connection. If the client system does not submit the Logon message within 60 seconds, the TCP/IP socket connection is assumed to be stale and the socket is closed.

See also: Session Layer - Fault Tolerance for a discussion of setting the Fault Tolerance Indicator (FTI) at logon and failover scenarios.

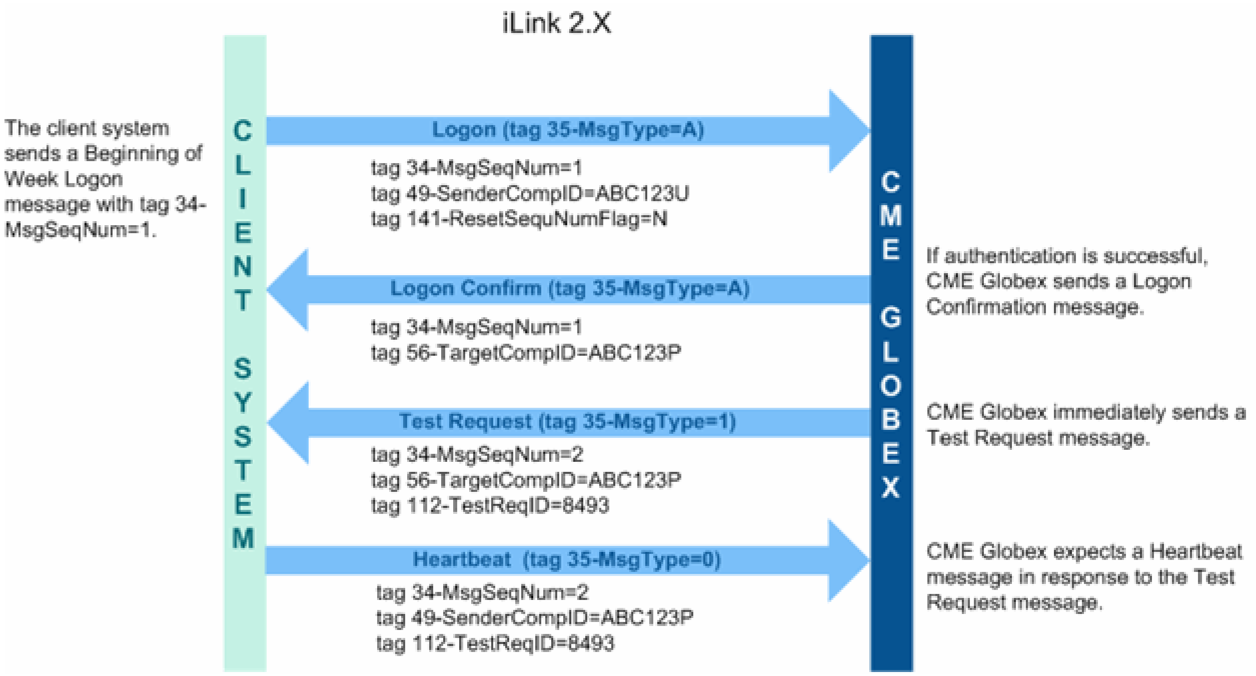
Beginning of Week Logon

The Beginning of Week Logon message must be populated with:

- Tag 49-SenderCompID with the Fault Tolerance Indicator set to 'U' for customers using Fault Tolerance or 'N' for customers opting not to use Fault Tolerance. This tag is 7 characters long and consists of 3 sub-fields:
  - Session ID (left-most 3 characters)
  - Firm ID (next 3 characters)
  - Fault Tolerance Indicator (last trailing character)
- Tag 141-ResetSeqNumFlag is optional but a Logon message with 141=Y will result in a Logout message response.
- Tag 34-MsgSeqNum = '1'

> ⓘ The Session ID and Firm ID are assigned and can be obtained by contacting your Global Account Manager.

The following diagram illustrates the message flow for a successful Beginning of Week logon scenario initiated by the client system.


iLink 2.X
CLIENT SYSTEM
CME GLOBEX
The client system sends a Beginning of Week Logon message with tag 34-MsgSeqNum=1.
Logon (tag 35-MsgType=A)
tag 34-MsgSeqNum=1
tag 49-SenderCompID=ABC123U
tag 141-ResetSequNumFlag=N
If authentication is successful, CME Globex sends a Logon Confirmation message.
Logon Confirm (tag 35-MsgType=A)
tag 34-MsgSeqNum=1
tag 56-TargetCompID=ABC123P
CME Globex immediately sends a Test Request message.
Test Request (tag 35-MsgType=1)
tag 34-MsgSeqNum=2
tag 56-TargetCompID=ABC123P
tag 112-TestReqID=8493
CME Globex expects a Heartbeat message in response to the Test Request message.
Heartbeat (tag 35-MsgType=0)
tag 34-MsgSeqNum=2
tag 49-SenderCompID=ABC123P
tag 112-TestReqID=8493

If any of the requirements are not met or if CME Globex is unable to authenticate the client system, the client system receives a iLink 2 Logout message and the connection is dropped. In addition, CME Globex does not increment its inbound sequence number.

If authentication is successful, a Logon Confirmation (tag 35-MsgType=A) message is sent with a Fault Tolerance Indicator of either 'P' or 'B' for customers using Fault Tolerance, or 'N' for customers opting not to use Fault Tolerance. The Fault Tolerance Indicator dictates whether the client application must behave as Primary (P) or Backup (B).

After sending the Logon Confirmation (tag 35-MsgType=A) message, CME Globex issues a iLink 2 Test Request message and expects a iLink 2 Heartbeat in response. The client application must receive the Logon Confirmation (tag 35-MsgType=A) message prior to sending the Heartbeat (tag 35-MsgType=0) message and any other subsequent messages.

Tag 141-ResetSeqNumFlag is optional but a Beginning of Week Logon message with 141=Y will result in a Logout message response.

Sequence Numbers - If the client system outbound* sequence number is not reset to '1' prior to the Beginning of Week Logon, and the client system sends a Logon (tag 35-MsgType=A) message, the client is logged out. **The logout message will have the following in tag 58-Text**=*Failed to reset sequence numbers at beginning of the week. Logout forced*. **The client must then reset sequence numbers and reattempt the logon**.

top

Mid-Week Logon

Mid-Week Logon is used for any subsequent logon after a successful Beginning of Week Logon. The Mid-Week Logon uses a sequence number series that continues from the next sequence number where the client logged off or was disconnected.

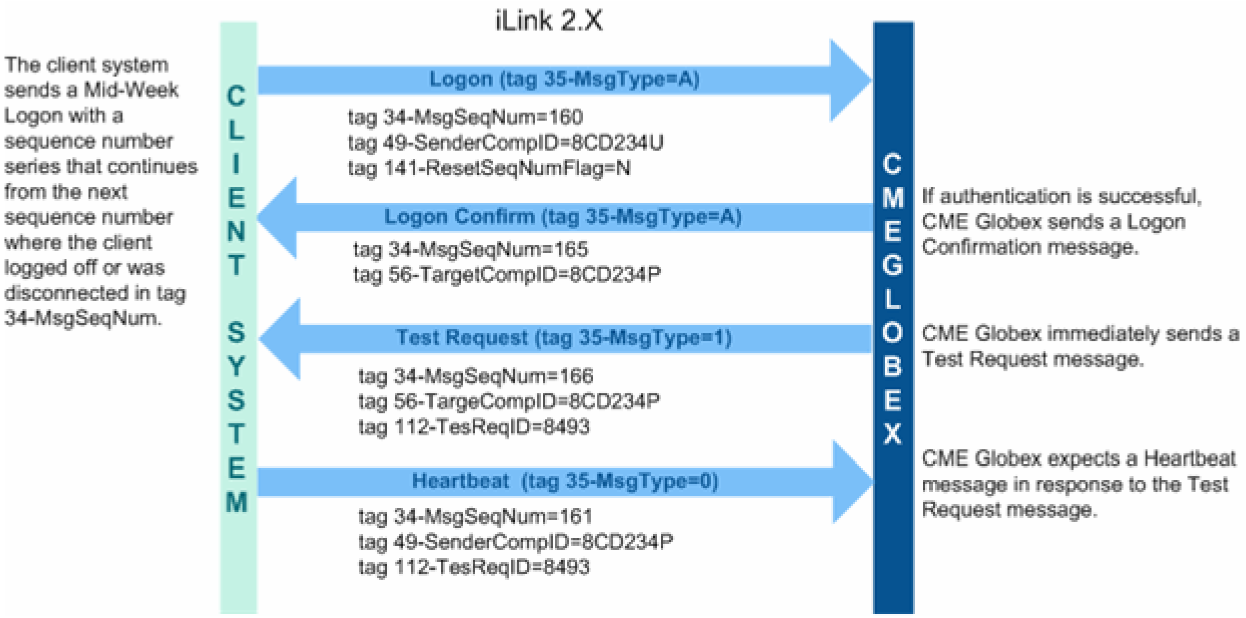
As a result, the Mid-Week Logon cannot have a sequence number set to '1'. The requirements of Mid-Week Logon are similar to the Beginning of Week Logon except for the sequence number requirement.

The requirements on the Mid-Week Logon message are:

- Tag 49-SenderCompID with the Fault Tolerance Indicator set to 'U' or 'N' for customers opting not to use Fault Tolerance.
- Tag 34-MsgSeqNo set to continue where the sequence left off at logout
- Tag 141-ResetSeqNumFlag is optional but a Mid-Week Logon message with 141=Y will result in a Logout message response.

If any of the above requirements are not met, the client system receives a iLink 2 Logout message in response. In addition, CME Globex does not increment its inbound sequence number.

The following diagram illustrates the message flow for a successful Mid-Week Logon scenario initiated by the client system.


iLink 2.X
CLIENT SYSTEM
CME GLOBEX
The client system sends a Mid-Week Logon with a sequence number series that continues from the next sequence number where the client logged off or was disconnected in tag 34-MsgSeqNum.
Logon (tag 35-MsgType=A)
tag 34-MsgSeqNum=160
tag 49-SenderCompID=8CD234U
tag 141-ResetSeqNumFlag=N
Logon Confirm (tag 35-MsgType=A)
tag 34-MsgSeqNum=165
tag 56-TargetCompID=8CD234P
If authentication is successful, CME Globex sends a Logon Confirmation message.
Test Request (tag 35-MsgType=1)
tag 34-MsgSeqNum=166
tag 56-TargeCompID=8CD234P
tag 112-TesReqID=8493
CME Globex immediately sends a Test Request message.
Heartbeat (tag 35-MsgType=0)
tag 34-MsgSeqNum=161
tag 49-SenderCompID=8CD234P
tag 112-TesReqID=8493
CME Globex expects a Heartbeat message in response to the Test Request message.

top

Mid-Week Logon and Undelivered Messages

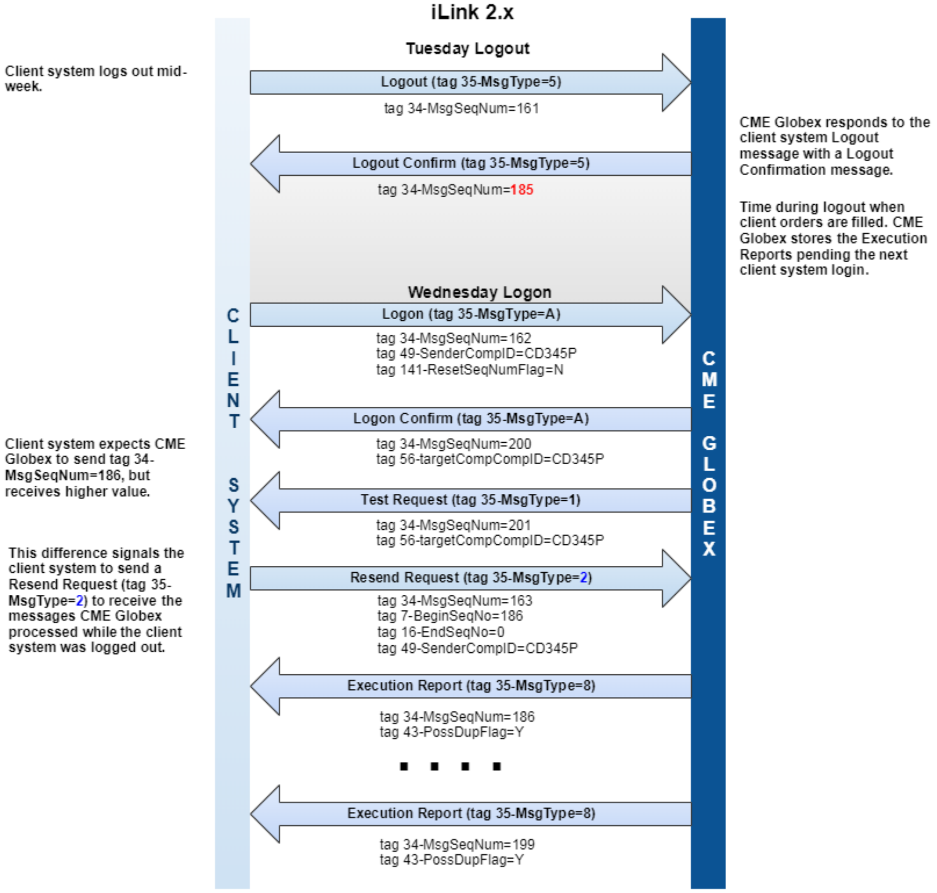
Mid-Week Logon provides handling for undelivered messages which were sent while the client system was logged out:

1. While the client system is logged out, CME Globex stores any messages to be sent to the client system.
2. As a result, the client system may receive a Logon Confirmation (tag 35-MsgType=A) message with a sequence number higher than expected due to the fact that CME Globex processed those stored messages prior to the Mid-Week Logon message and incremented its outbound sequence number accordingly.
3. The client system submits a iLink 2 Resend Request message for messages stored while the client system was logged out.

The following diagram illustrates the message flow for a Mid-Week Logon scenario where undelivered Execution Reports messages were generated by the CME Globex platform while the client system was logged out.

1. The client system successfully logged on Tuesday morning and submitted New Order Request (tag 35-MsgType=D) messages.
2. The client system logged out. While the client system is logged out, the orders remain active and any corresponding Execution Reports are generated. CME Globex processes these Execution Reports and increments its outbound sequence number while the client system is logged out.
3. The client system logs in on Wednesday morning. When the client system receives the Logon Confirmation (tag 35-MsgType=A) message, the client system detects that the sequence number of the Logon Confirmation (tag 35-MsgType=A) message is higher than expected. The client application follows up with a Resend Request (tag 35-MsgType=2) message and retrieves unsent messages that were generated while the client system was logged out.

The following diagram illustrates the message sequence for a Mid-Week Logon with unsent messages where the client system logs off and logs back on during mid-week.


iLink 2.x
Tuesday Logout
Client system logs out mid-week.
Logout (tag 35-MsgType=5)
tag 34-MsgSeqNum=161
CME Globex responds to the client system Logout message with a Logout Confirmation message.
Logout Confirm (tag 35-MsgType=5)
tag 34-MsgSeqNum=185
Time during logout when client orders are filled. CME Globex stores the Execution Reports pending the next client system login.
Wednesday Logon
Logon (tag 35-MsgType=A)
tag 34-MsgSeqNum=162
tag 49-SenderCompID=CD345P
tag 141-ResetSeqNumFlag=N
CLIENT SYSTEM
CME GLOBEX
Logon Confirm (tag 35-MsgType=A)
tag 34-MsgSeqNum=200
tag 56-targetCompCompID=CD345P
Client system expects CME Globex to send tag 34-MsgSeqNum=186, but receives higher value.
Test Request (tag 35-MsgType=1)
tag 34-MsgSeqNum=201
tag 56-targetCompCompID=CD345P
This difference signals the client system to send a Resend Request (tag 35-MsgType=2) to receive the messages CME Globex processed while the client system was logged out.
Resend Request (tag 35-MsgType=2)
tag 34-MsgSeqNum=163
tag 7-BeginSeqNo=186
tag 16-EndSeqNo=0
tag 49-SenderCompID=CD345P
Execution Report (tag 35-MsgType=8)
tag 34-MsgSeqNum=186
tag 43-PossDupFlag=Y
. . . .
Execution Report (tag 35-MsgType=8)
tag 34-MsgSeqNum=199
tag 43-PossDupFlag=Y

top

In-Session Logon

Warning

In-Session Logon should only be used to recover from catastrophic failure, since all messages sent prior to the reset will not be recoverable..

The client system must send a Test Request (tag 35-MsgType=1) message before sending an In-Session Logon (tag 35-MsgType=A) message. If not sent in that order, the client system may lose messages that cannot be requested again as the sequence number may be reset to '1' for both parties, client and CME Globex.

In-Session Logon is used to reset sequence numbers after the client has logged on. During In-Session Logon, tag 141-ResetSeqNumFlag must be set to 'Y' to reset sequence numbers and tag 34-MsgSeqNum of that Logon must be set to '1'. If the client would like to reset sequence numbers in the middle of a session, the client should follow these steps:

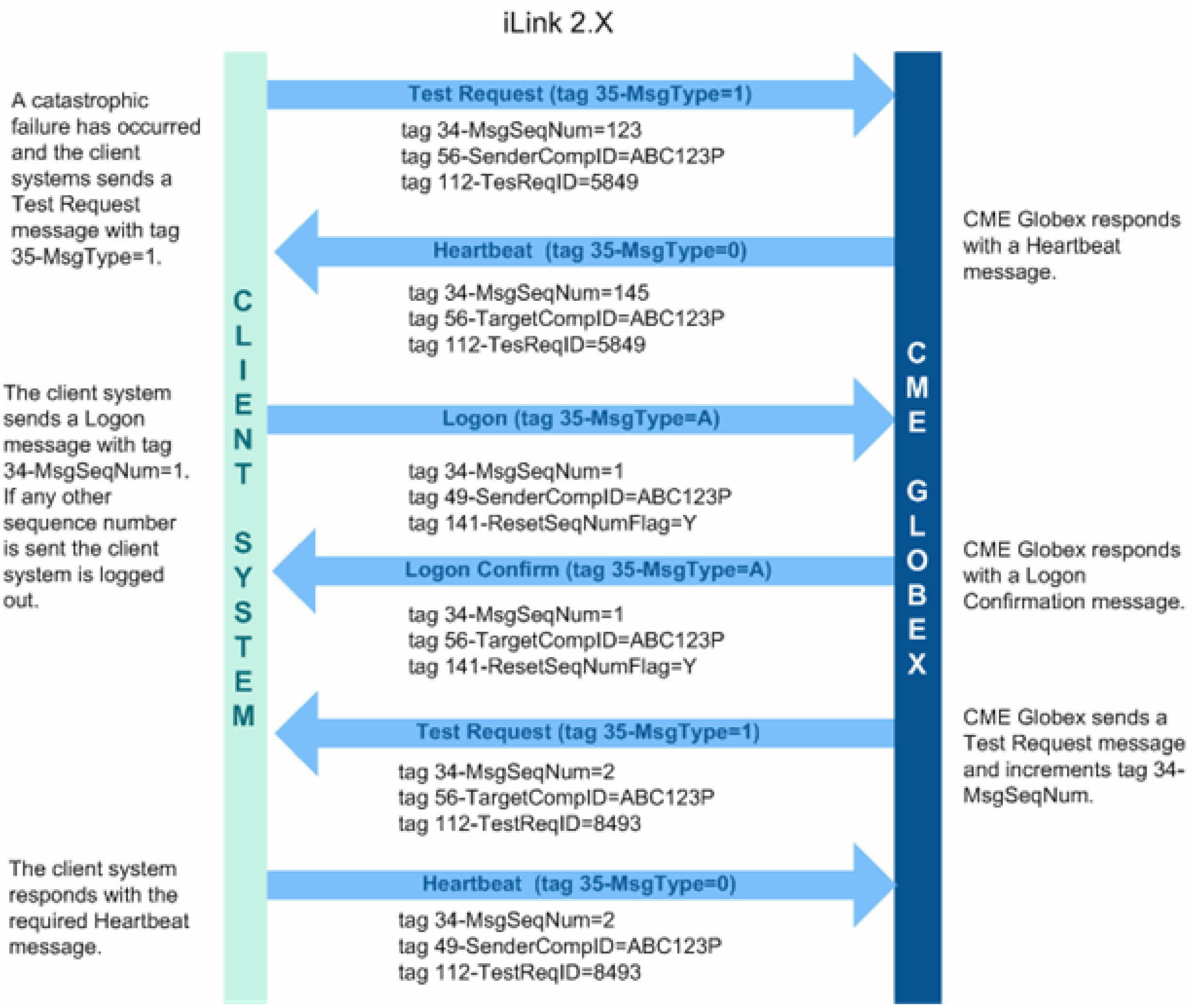
1. Send a iLink 2 Test Request message and wait for a iLink 2 Heartbeat message to ensure that there are no sequence number gaps.
2. Send a Logon (tag 35-MsgType=A) message with tag 141-ResetSeqNumFlag set to 'Y' and a sequence number of '1' in tag 34-MsgSeqNum.
   - If the client system sends an In-Session Logon (tag 35-MsgType=A) with tag 141-ResetSeqNumFlag set to 'N' or if the tag is missing, then the client system is logged out.
   - In addition, if the client sends a sequence number other than '1' in tag 34-MsgSeqNum during In-Session Logon, the client system is logged out.
3. CME Globex responds with a Logon Confirmation (tag 35-MsgType=A) message with tag 141-ResetSeqNumFlag set to 'Y' and a sequence number of '1' in tag 34-MsgSeqNum.

CME Globex resets its inbound and outbound sequence numbers and expects the client's subsequent message to have a sequence number of '2'.

Do not use tag 141-ResetSeqNumFlag to recover from network disconnects during the week.

In-Session Logon Used to Reset Sequence Number

The following diagram illustrates a successful In-Session Logon scenario where the client system uses a iLink 2 Test Request message and resets sequence numbers to '1' due to a catastrophic failure.



A catastrophic failure has occurred and the client systems sends a Test Request message with tag 35-MsgType=1.

Test Request (tag 35-MsgType=1)

tag 34-MsgSeqNum=123
tag 56-SenderCompID=ABC123P
tag 112-TesReqID=5849

CME Globex responds with a Heartbeat message.

Heartbeat (tag 35-MsgType=0)

tag 34-MsgSeqNum=145
tag 56-TargetCompID=ABC123P
tag 112-TesReqID=5849

The client system sends a Logon message with tag 34-MsgSeqNum=1. If any other sequence number is sent the client system is logged out.

Logon (tag 35-MsgType=A)

tag 34-MsgSeqNum=1
tag 49-SenderCompID=ABC123P
tag 141-ResetSeqNumFlag=Y

CME Globex responds with a Logon Confirmation message.

Logon Confirm (tag 35-MsgType=A)

tag 34-MsgSeqNum=1
tag 56-TargetCompID=ABC123P
tag 141-ResetSeqNumFlag=Y

CME Globex sends a Test Request message and increments tag 34-MsgSeqNum.

Test Request (tag 35-MsgType=1)

tag 34-MsgSeqNum=2
tag 56-TargetCompID=ABC123P
tag 112-TestReqID=8493

The client system responds with the required Heartbeat message.

Heartbeat (tag 35-MsgType=0)

tag 34-MsgSeqNum=2
tag 49-SenderCompID=ABC123P
tag 112-TestReqID=8493

top