BellSouth Interconnection Services
675 West Peachtree Street
Atlanta, Georgia 30375

Carrier Notification
SN91082688

Date: October 31, 2001

To: Competitive Local Exchange Carriers (CLECs)

Subject: CLECs - Telecommunications Access Gateway (TAG) Security Guidelines

BellSouth is committed to improving the overall performance of interfaces utilized by the CLECs. As part of that effort, BellSouth has discovered an apparent misunderstanding on the part of certain users of the TAG interface as it relates to security credentials. This misunderstanding has increased the transaction response timeliness of TAG and has adversely affected all TAG users.

To address this issue, BellSouth has adopted the attached "TAG Security Guidelines." These guidelines will become effective on January 6, 2002. CLECs should begin making any necessary coding and administrative changes to comply. BellSouth is prepared to provide technical assistance to any CLEC making the requisite coding and administrative changes or to answer any questions concerning the TAG Security Guidelines.

BellSouth will continue to make enhancements to the interfaces utilized by the CLECs. Your assistance in this matter is appreciated.

Please contact your BellSouth account team manager or Software Vendor Certification Manager for questions or to arrange for TAG technical support and/or testing.

Sincerely,

ORIGINAL SIGNED BY JIM BRINKLEY

Jim Brinkley – Senior Director
BellSouth Interconnection Services

TELECOMMUNICATION ACCESS GATEWAY (TAG)
SECURITY GUIDELINES

Purpose

The purpose of this document is to define a set of rules that Competitive Local Exchange Carriers (CLECs) should use in coding their TAG applications with regards to the appropriate use of security credentials.

These rules are designed to promote the re-use of security credentials for the benefit of all CLECs. Security overhead increases the time it takes CLECs to process transactions via TAG, while re-using security credentials reduces transaction response timeliness. A CLEC's failure to re-use security credentials also adversely impacts other CLECs, since the Security Server components within TAG are involved in every single transaction, in effect, creating a limited resource within the TAG point of entry. The unnecessary processing required by the Security Server when credentials are not re-used increases turnaround time through these components for all CLECs including those that do re-use credentials.

Scope

The rules apply to all TAG Application Program Interface (API) versions.

Rules for CLEC TAG Applications

1. TAG objects, once created and credentialed, should be re-used rather than re-created for at least sixty minutes following first use.[1]

2. A TAG object, once created and credentialed, should not relinquish its credentials if they will be needed again within sixty minutes of first use.

3. For at least the first sixty minutes of a credentialed TAG Object's life, a CLEC application should use that object for any request requiring the same TAG Object Class, if the object is currently available, rather than creating and or credentialing another object of that class.

4. TAG objects should be re-credentialed only in response to Security Exceptions rather than at some arbitrary time interval. This should be done on an object-by-object basis, as each individual object receives the Security Exception.

5. CLEC TAG applications should employ an on-demand protocol for both creating and credentialing TAG objects such that an object is not created, credentialed, or re-credentialed until a transaction is ready to submit through that object.

[1] In Rules 1, 2, 3 and 7, sixty minutes is the minimum recommendation for object re-use. CLECs are encouraged to re-use objects for the entire duration of their programs.

6. CLEC TAG applications should enforce an upper bound on the number of TAG objects of the same TAG Object Class that can exist concurrently within the application such that the number of TAG objects of the same class does not exceed the number reasonably needed by the application. The number needed can be calculated using the method shown below. This calculation should be predicted in advance based on historical experience and future assumptions.

   Max Objects = *Transaction Rate* / *Object Throughput*

   Where
   Transaction Rate is the total number of transactions of a single Object Class type expected to be submitted using that application id over a certain *Time Period*, and

   Object Throughput = *Time Period* / *Transaction Response Interval*

   Where
   Time Period is the same interval used to calculate *Max Objects*, and
   Transaction Response Interval is the expected interval between submission and response times for this Object Class.

   Note: BellSouth can provide expected intervals for each Object Class from time of receipt by BellSouth to return of response by BellSouth, at the TAG boundaries. The CLEC must estimate and add: a) expected network transmission time; and b) any additional processing time within its application, in order to estimate *Transaction Response Interval* accurately.

7. CLEC TAG applications should not destruct a credentialed TAG object within the first sixty minutes following its first use unless the CLEC TAG application is terminating.

8. When terminating, CLEC TAG applications should destruct all of the TAG objects they created during execution.

Definitions

1. TAG Object – An instantiation of any of the pre-order or firm-order classes provided by the TAG API.

2. Creating a TAG Object – Invoking the constructor method for any of the pre-order or firm-order classes provided by the TAG API

3. Credentialing a TAG Object – Automatically done once by a TAG Object the first time any of the transaction submission methods within a created TAG Object are invoked.

4. Re-credentialing a TAG Object – Automatically done by a previously-credentialed TAG Object the first time any of its transaction submission methods are invoked immediately after one of the following method calls for that Object has been made:

- applicationId
- applicationPassword
- surrenderCredentials
- routingInfo

Exception Handling

There are five types of Security Exceptions raised by the API that can be associated with re-using TAG Objects/credentials:

- No Prior Authentication
- Cookie Expired
- Security Violation Detected
- Cookie Invalid
- Inactivity Detected.

Definitions are provided below for each of these Security Exceptions. For all five of these, the CLEC Application should take the following action:

1. Reset the value for either applId or applPassword using the Object's "applicationId" or "applicationPassword" methods respectively, and

2. Reinitiate the Object's method call that originally caused the exception.

When the reinitiated API call is made, TAG will detect that the application id or application password has been modified and will automatically attempt to reacquire credentials for the object prior to proceeding with the request.

Note: A CLEC application should not try more than two successive, unsuccessful attempts to reacquire credentials because three unsuccessful attempts to reacquire credentials will result in the disabling of the CLEC's application id.

No Prior Authentication: No credentials exist for the object making the request. This could be caused by a failure recovery process in the BellSouth TAG Server.

Cookie Expired: Credentials provided to an object at construction time have exceeded the maximum lifetime configured for objects of that Class. Currently this value is set to twenty-four hours.

Security Violation Detected: Credentials reference an object that does not exist or has been disabled. This could be caused by a failure recovery process in the BellSouth TAG Server.

Cookie Invalid: Credentials provided to an object at construction are not valid in the targeted TAG environment. This could be caused by a failure recovery process in the BellSouth TAG Server.

Inactivity Detected: Credentials provided to an object at construction time have not been used for a period that exceeds the maximum inactivity interval configured for objects of this Class. Currently this value is set to 60 minutes (1 hour).

No Prior Authentication: No credentials exist for the object making the request. This could be caused by a failure recovery process in the BellSouth TAG Server.

CLEC Application Testing

As part of their TAG Profile, each CLEC must provide the Max Objects value for each TAG pre and firm order class it intends to implement. As part of testing, BellSouth may ask the CLEC to perform the following three-step test for each class being tested:

1. Submit a continuous or near-continuous series of transactions associated with the class, where series is one more than the Max Objects specified by the CLEC for that class. The number of TAG Objects created by the CLEC (as evidenced by BellSouth TAG Trace and Log Files) should not exceed Max Objects.

2. Following 55 minutes of idle time for the CLEC Application, the CLEC will re-submit the same stream of transactions. No credentialing or re-credentialing of any TAG objects by the CLEC Application should be observed and the application should exclusively re-use previously created and credentialed objects.

3. The CLEC will bring down its application. This should result in all objects created by the CLEC Application surrendering their credentials.

BellSouth Monitoring During Production

In monitoring Security Server performance, BellSouth may monitor CLEC TAG transactions in the production environment to ensure compliance with the TAG Credential Rules. In order to protect all CLECs using TAG, BellSouth reserves the right to suspend any CLEC that is found in noncompliance with the TAG Credential Rules from further use of TAG until adherence to the TAG Credential Rules can be demonstrated by the CLEC and verified by BellSouth in a BellSouth test environment.