AS2 Communication Guidelines and Golli

This page lists GS1 spesification http://www.gs1.org/docs/xml/EDIINT_AS1_AS2_Transport_Comm_Guide_i1.pdf requirements and recommendations and defines what is status of Golli implementation against it.

Golli implementation of AS2 protocol is based on OpenAS2 implementation.

Requirements

Category	Requirement	Golli implementation	Notices etc.
Encryption and Signature Requirements	Requirement 1: Payload data SHALL be encrypted and digitally signed using the S/MIME specification (see RFC 3851).	✅ Golli uses signing and encryption. To implement SMIME Golli uses Bouncy Castle	
	Requirement 2: The length of the one-time session (symmetric) key SHALL be 128 bits or greater. Note: Key lengths less than 128 bits are no longer considered secure. Triple DES, which uses 3 separate 56 bit keys to encrypt the data three times, is the recommended encryption algorithm. A newer algorithm called Advanced Encryption Standard (AES), while not currently used for EDIINT encryption, was developed under the National Institute of Standards and Technology leadership and supports key sizes of 128, 192, and 256 bits. AES is used by the US government and it is expected that it will be widely used by business applications in the future. There may be export or import restrictions affecting use of encryption technologies in a few countries. See http://www.bis.doc.gov/Encryption/Default.htm	✅Golli supports Triple DES with 192 (168) bit key. (des_EDE3_CBC)	
	Requirement 3: The length of the Public/Private Encryption key SHALL be 1024 bits or greater. Note: Key length options for public/private keys are: 512, 1024, or 2048 bits.	✅ Golli will use keys of 2048 bits.	
	Requirement 4: The length of the Public/Private Signature key SHALL be 1024 bits or greater.	✅ Golli will use keys of 2048 bits.	
	Requirement 5: The Signature Hash algorithm used SHALL be SHA1. Note: SHA1 is considered a significantly stronger algorithm for creating document digests used for digital signatures than the MD5 algorithm.	✅ Golli supports SHA1 for signature hashes.	
Configuration Requirement	Requirement 6: Digitally signed receipts (Signed Message Disposition Notifications [MDNs]) SHALL be requested by the Sender of Message (see Glossary). Note: MDNs provide a guarantee to the sender that the message has been received and the recipient has signed an acknowledgment	✅ Golli supports signed MDN:s	

Recommendations

Recommendation	Golli implementation	Notices et.
Recommendation 1 – MDN Request Option Either Asynchronous or Synchronous MDNs MAY be used with EDIINT AS2. There are potential issues with both synchronous and asynchronous MDNs, and Trading Partners need to jointly determine which option is best based on their operational environments and message characteristics. A discussion of both options follows these recommendations. Note: For EDIINT AS1, MDNs are always asynchronous, since SMTP (email) does not support bi-directional transmission.	✅ Golli supports both async /sync MDN as response (although only synchronous is tested and also recommended to be used). Golli itself requests MDN always as synchronous.	
Recommendation 2 – MDN Delivery Recipients SHOULD transmit the MDN as soon as technically possible to ensure that the message sender recognizes that the message has been received and processed by the receiving EDIINT software in a timely fashion. This applies equally to AS1 and AS2 as well as Asynchronous and Synchronous MDN requests.	✅ Golli sends MDN as soon as message is received, decrypted, signature verified and written to database.	
Recommendation 3 – Delivery Resend with Asynchronous MDNs Requested When a message has been successfully sent, but an asynchronous MDN has not been received in a timely manner, the Sender of Message SHOULD wait a configurable amount of time and then automatically resend the original message. A delivery resend of a message SHALL have the same content and the same Message-ID value as the initial message. The period of time to wait for a MDN and then automatically resend the original message is based on business and technical needs, but generally SHOULD not be less than one hour. There SHOULD be no more than two automatic resends of a message before personally contacting a technical support contact at the Receiver of Message site. This applies equally to AS1 and AS2.	❌ Golli uses synchronous MDNs when sending. So there is no need to implement this.	

Recommendation 4 – Delivery Retry for AS2 Delivery retry SHOULD take place when any HTTP response other than “200 OK” is received (for example, 401, 500, 502, 503, timeout, etc). This occurrence indicates that the actual transfer of data was not successful. A delivery retry of a message SHALL have the same content and the same Message-ID value as the initial message. Retries SHOULD occur on a configurable schedule. Retrying SHALL cease when a message is successfully sent (which is indicated by receiving a HTTP 200 range status code), or SHOULD cease when a retry limit is exceeded.	✅ Golli is capable of trying resending messages. Amount of retries and delay between those can be configured on system level (not by organization).	
Recommendation 5 – Message Resubmission If neither automated Delivery Retry nor automated Delivery Resend are successful, the Sender of Message MAY elect to resubmit the payload data in a new message at a later time. The Receiver of Message MAY also request message resubmission if a message was lost subsequent to a successful receive. If the message is resubmitted a new Message-ID MUST be used. Resubmission is normally a manual compensation.	TODO this need to be handle case by case if needed. No automatic support for this.	
Recommendation 6 – HTTP vs. HTTP/S (SSL) For EDIINT AS2, the transport protocol HTTP SHOULD be used. However, if there is a need to secure the AS2-To and the AS2-From addresses and other AS2 header information, HTTPS MAY be used in addition to the payload encryption provided by AS2. The encryption provided by HTTPS secures only the point to point communications channel directly between the client and the server. Note: HTTPS might introduce operational complexities.	✅ Golli supoorts http for AS2 as recommended	
Recommendation 7 – AS2 Header For EDIINT AS2, the values used in the AS2-From and AS2-To fields in the header SHOULD be GS1 Global Location Numbers (GLNs). Note: The GLNs SHOULD be that of the sending server and receiving server respectively. When a hub or VAN is used, the GLN of the trading partner MAY be used when the AS2 To field is used for routing. Existing AS2 installations using values other than GLNs would need to reconfigure their software and coordinate with all of their trading partners prior to converting to the use of GLNs.	❌ Golli doesn't force GLN. Golli works as router and there are two hardcoded names for golli instances. Other parties can choose their AS2 id as they wish as long as it is unique in Golli. GLN is of course preferred as GS1 recommends.	
Recommendation 8 - SMTP For EDIINT AS1, a dedicated SMTP server, separate from the normal email server SHOULD be used to ensure operational reliability.	❌ Golli not support AS1	
Recommendation 9 - Compression EDIINT compression MAY be used as an option, especially if message sizes are larger than 1MB. Although current versions of EDIINT software handle compression automatically, this SHOULD be bilaterally agreed between the sender and the receiver. Note: If used, compression SHOULD comply with the IETF document “Compressed Data for EDIINT” http://www.ietf.org/internet-drafts/draft-ietf-ediint-compression-05.txt	❌ Compression not used	
Recommendation 10 – Digital Certificate Characteristics Digital certificates MAY either be from a trusted third party or self signed if bilaterally agreed between trading partners. If certificates from a third party are used, the trust level SHOULD be at a minimum what is termed ‘Class 2’ which ensures that validation of the individual and the organisation has been done.	✅ Golli can use either self signed or trusted certificate.	TODO Discussion of self signed vs CA signed certificates? Basically in AS2 certificates are always exchanged and trust chain is not in that important role that it is in e. g. HTTPS where browser has CA certificates to trust and remote server identity is verified by using trust chain (server certificate is signed by trusted party which already exists in browser). Anyway Golli needs signed certificate for https so it is possible to take those now in use also in AS2 when they are arrived. Anyhow I would not to force all participants to use 3rd party trusted certificates because it probably won't make any difference and it would cost.
Recommendation 11 – Common Digital Certificate for Encryption & Signature A single digital certificate MAY be used for both encryption and signatures, however if business processes dictate, two separate certificates MAY be used. Although current versions of EDIINT software handle two certificates automatically, this SHOULD be bilaterally agreed between the sender and the receiver.	❌ Golli is not supporting separate certificates for signing and encryption. Common certificate is used for both.	Is some partner really using separate certificates for signing and encryption?

Recommendation 12 – Digital Certificate Validity Period The minimum validity period for a certificate SHOULD be 1 year. The maximum validity period SHOULD be 5 years.	✅ This is about certificate creation. Golli implementation doesn't restrict this.	TODO If really wanted it probably is possible to make software restrictions to this which forbid on code level of usage of certificate which doesn't obey this.
Recommendation 13 – Digital Certificate – Automated Exchange The method for certificate exchange SHALL be bilaterally agreed upon. When the Certificate Exchange Messaging for EDIINT specification is widely implemented by software vendors, its use will be strongly recommended. This IETF specification will enable automated certificate exchange once the initial trust relationship is established, and will significantly reduce the operational burden of manually exchanging certificates prior to their expiration. Note: See IETF document: https://datatracker.ietf.org/public/idindex.cgi?command=id_detail&id=12703	❌ Golli is not supporting this	This is not discussed. Is some partner supporting this kind of automatic certificate exchange?
Recommendation 14 – HTTP and HTTP/S Port Numbers for AS2 Receiving AS2 messages on a single port (for each protocol) significantly minimizes operational complexities such as firewall set-up and potential security exposures for both the sending and receiving partner. Ideally, all AS2 partners would receive messages using the same port number. However some AS2 partners have previously standardized to use a different port number than others and changing to a new port number would add costs without commensurate benefits. Therefore AS2 partners MAY standardize on the use of port 4080 to receive HTTP messages and the use of port 5443 to receive HTTP/S (SSL) messages.	❌ Golli is not forcing or standardizing any port numbers. Remote AS2 urls may be anything remote side want's to use (configuration). On Golli side normal http/https ports will be used.	
Recommendation 15 – Duplicate AS2 Messages AS2 software implementations SHOULD use the 'AS2 Message-ID' value to detect duplicate messages and avoid sending the payload from the duplicate message to internal business applications. The Receiver of Message SHALL return an appropriate MDN even when a message is detected as a duplicate. Note: The Internet Engineering Task Force (IETF) is developing an Operational Reliability for EDIINT AS2 specification which defines procedures to avoid duplicates and ensure reliability. Note: See IETF document: https://datatracker.ietf.org/public/idindex.cgi?command=id_detail&id=13578	✅ Golli omits message if golli already has message with same id in database. Golli still replies to sender with valid MDN.	
Recommendation 16 – Technical Support There SHOULD be a technical support contact for each Sender of Message and Receiver of Message. The contact information SHOULD include name, email address and phone number. For 24x7x365 operation, a pager or help desk information SHOULD be also provided.	TODO probably need to be discussed Golli will contain some info of organizations. E.g. name. There might be need to add even more. Also organizations will have admin users which will have email as username. We already has had some thoughts about sending emails in failure cases, but might be need to be discussed which is correct point of contact for those. So this needs further discussion.	