# EASEE-gas

European Association for the Streamlining of Energy Exchange - gas

# Common Business Practice

Number: 2017-002/01

Subject: Secure communication over the internet

Approved: 10-07-2017

## Summary

This Common Business Practice specifies the method to safely setup connections over the internet for sharing information.

## About EASEE-gas

*The European Association for the Streamlining of Energy Exchange-gas or EASEE-gas was created by six founding members in Paris on March 14th, 2002. EASEE-gas' aim is to support the creation of an efficient and effective European gas market through the development and promotion of common business practices (CBPs) that intend to simplify and streamline business processes between the stakeholders.*

*The formation of EASEE-gas was prompted by the success of the Gas Industry Standards Board in the United States and has been modelled on it. The GISB has now evolved into the North American Energy Standards Board. The creation of EASEE-gas is a project that is fully supported by the European Commission and by the European Regulators through the so-called Madrid Forum. It was achieved through the work of a dedicated Task Force supported by EFET, Eurogas, Eureectric, GEODE, GTE, OGP and the Edigas group.*

*The association is fundamentally based on company membership and voluntary contribution towards the development of common business practices.*

*Full membership in EASEE-gas is open to all companies, European or other, that are involved in the European gas business, from producers to end users, and to companies that are their service providers. Companies can subscribe to full membership in one or more of the eight gas industry segments.*

*Associate membership in EASEE-gas is open to government agencies, e.g., regulators, through to organisations such as gas business trade associations and to individuals that may contribute to the benefit of EASEE-gas. Associate members do not pay annual fees, nor do they have voting rights.*

*The development of common business practices within EASEE-gas is organised through working groups under the supervision of an executive committee that is representative of the various gas industry segments. Participation in the working groups is limited to members only.*

# Common Business Practice 2017-002/01: "Secure communication over the internet"

## 1. APPLICATION AREA

The adoption of this Common Business Practice means that EASEE-gas members will use the proposed standard for secure messaging.

Use at least TLS v1.2 for securing internet communication.

The main focus is the document exchange in business processes, which means machine-to-machine communication. In general the use of TLS v1.2 should be considered for all communications.

## 2. MANAGEMENT SUMMARY

The time to migrate is now, security is important. The overall security of the gas data exchange must be on the right level, the weakest link can jeopardise all market participants.

For over 20 years Secure Sockets Layer (SSL) has been in the market as one of the most widely-used encryption protocols ever released, and remains in widespread use today despite various security vulnerabilities exposed in the protocol.
Fifteen years ago, SSL v3.0 was superseded by TLS v1.0 (TLS=Transport Layer Security), which has since been superseded by TLS v1.1 and v1.2. To date, SSL and early TLS no longer meet minimum security standards due to security vulnerabilities in the protocol for which there are no fixes. Attacks such as DROWN, POODLE and BEAST make active use of those vulnerabilities. Relevant information can be found in the CVE database [CVE]

It is critically important that parties upgrade to a secure alternative as soon as possible, and disable any fall back to both SSL and early TLS.

This CBP wants to set the minimum requirements for secure communications.
To do this any protocol lower then TLS v1.2 must be disabled, systems must be configured so that no fall back to early TLS or SLL is possible. Also a recommendation will be made for secure ciphers to ensure interoperability.

## 3. IMPLEMENTATION DATE

The implementation of this CBP shall be before the end of 2017 or as soon as practical. In practice parties should check if their counterparties support TLS v1.2 with the selected cipher suites. As soon as all counterparties can connect using TLS v1.2 a participant can switch to TLS v1.2 only.

## 4. TECHNOLOGY TO BE USED

SSL/TLS is a suite of protocols. The best practice for transport layer protection is to only provide support for the TLS protocol, and specifically TLS v1.2. Currently there is no higher operational protocol, but over time protocols evolve to keep up with security and higher versions are expected (TLS v1.3 is in draft). The sole use of TLS v1.2 and higher will provide maximum protection against skilled and determined attackers and is appropriate for applications handling sensitive data or performing critical operations. However, this technology should be constantly reviewed.

TLS v1.2 provides modern cryptographic algorithms, the cipher suites, there is support for over 300 suites. The strength of the encryption used within a TLS session is determined both by the key exchange/agreement and the encryption cipher negotiated between endpoints. In order to ensure that only strong cryptographic ciphers are selected, a termination endpoint e.g. server, firewall, must be modified to disable the use of weak ciphers and to configure the ciphers in strength priority. It is recommended to configure the endpoint to only support strong ciphers and to use sufficiently large key sizes.

The technology is explained in chapter 7 "Technology talk".

### *Recommendations*

Currently not all systems/applications support the best cipher suites, therefore the list below is used for reference, it is however advised to migrate to the "considered safe" ciphers as recommended by ENISA and BSI. A yearly review of the usage of cipher suites is recommended.

**Cipher suites recommended, considered safe, set:**
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256

**Cipher suites classified not considered as safe, but currently acceptable:**
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA

## 5. PROCESS

In order to be ready before the end of 2017 EASEE-gas members are asked to share their readiness/planning with the TSWG.
Parties will use their testing or acceptance systems to determine the interoperability. Testing results must be consolidated and provided to the TSWG and published. See implementation plan and explanatory notes [CBP 2017-002-01-EX].

Parties that are ready can use TLS v1.2, this is regulated by the software itself on the basis of the negotiation between systems. Switching to a TLS v1.2 only situation can be done by individual parties if all communication parties support TLS v1.2.

## 6. DEFINITIONS

The terms, Secure Socket Layer (SSL) and Transport Layer Security (TLS) are often used interchangeably. In fact, SSL v3.1 is equivalent to TLS v1.0. However, different versions of SSL and TLS are supported by modern web browsers and by most modern web frameworks and platforms. For the purposes of this CBP we will refer to the technology generically as TLS for transport layer security.

## 7. TECHNOLOGY TALK

In this chapter the elements in the TLS protocol are explained.

### *Basic elements of a cipher suite*

The TLS protocol suite aims to provide a confidential channel in which the protocol is broken up into two phases: A handshake (or key agreement) phase and a record layer encryption phase, the total is described as a cipher suite. A cipher suite is basically a complete set of methods (technically known as algorithms) needed to secure a network connection through TLS (Transport Layer Security). The name of each set is representative of the specific algorithms comprising it.

There are four algorithms that make up a cipher suite. The algorithms that make up a typical cipher suite are the following:

- key exchange algorithm - dictates the manner by which symmetric keys will be exchanged;
- bulk encryption algorithm - dictates which symmetric key algorithm will be used to encrypt the actual data;
- Message Authentication Code (MAC) algorithm - dictates the method the connection will use to carry out data integrity checks;
- authentication or signature algorithm - dictates how server authentication and (if needed) client authentication will be carried out;

One cipher suite typically consists of 1 key exchange, 1 authentication, 1 bulk encryption, and 1 MAC algorithm. Some examples (with considerations based on [ENISAAKSP]):

- Key exchange algorithms: RSA, DH, ECDH, ECDHE, where RSA is doubtful but within TLS v1.2 still considered safe and DH is preferred;

- Authentication algorithms: RSA, DSA, ECDSA, where RSA key size is min. 2048 bits and ECDSA is preferred;
- Bulk encryption algorithms: AES, 3DES, CAMELLIA, where 3DES is not considered safe on the long term and AES-128 bit is the minimum in conjunction with GCM (CBC is not considered safe);
- MAC algorithms: SHA, MD5, where MD5 is not considered safe and SHA should be used with an output length of 256 bits or more.

An example of a typical cipher suite:
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

The breakdown is as follows:

- TLS simply indicates the protocol;
- ECDHE signifies the key exchange algorithm;
- ECDSA signifies the authentication algorithm;
- AES_256_CBC indicates the bulk encryption algorithm;
- SHA384 indicates the MAC algorithm.

AES_256_CBC means that this cipher suite specifically uses 256-bit AES operating in CBC (cipher block chaining) mode.

Similarly, SHA384 means the cipher suite is employing a specific version of the Secure Hash Algorithm (SHA).

### *Considerations*

TLS v1.2 is the only protocol supporting AEAD (Authenticated Encryption with Associated Data) which is needed to provide sufficient security.
Furthermore the Diffie-Hellman (DH) Key Agreement should be used. It is recommended to use Elliptic Curve (EC) type certificates, they are faster and less costly in terms of footprint than traditional RSA, the value is not to exceed 384 bits: Using a key that is too short is insecure, but using a key that is too long will result in "too much" security and slow operation in terms of CPU load. ECDSA is not widely supported due to potential patent issues.
To support a wider range of clients, companies should also enable DHE suites as fall back after ECDHE (the E at the end refers to ephemeral key exchange). There is little benefit to increasing the strength of the ephemeral key exchange beyond 2048 bits for DHE and 256 bits for ECDHE. There are no clear benefits of using encryption above 128 bit.
In the end, wide support of ciphers, security and performance are the basis of the choices for the cipher suites.

### *Reasoning*

The security guidance provided by ENISA is based on state-of-the-art best practices, following recommendations for "near term" (defined as "at least ten years") future system use. The guidance on the use of Transport Layer Security is published in the "ENISA Algorithms, Key Sizes and Parameters Report 2013" with an update in 2014

[ENISAAKSP] and in a "Mindest-standard" of the Federal Office for Information Security (BSI) [BSITLS].
The ENISA and BSI reports state that TLS v1.0 and TLS v1.1 should not be used. Older versions such as SSL v2.0 and SSL v3.0 must not be used. Implementations compliant with this CBP must therefore support TLS v1.2 [RFC5246].
IANA publishes a list of TLS cipher suites [TLSSP], only a subset of which the ENISA report considers safe (see [ENISAAKSP]). Implementations should support cipher suites included in this subset.
Support for cipher suites that are not currently considered secure should be disabled by default. Perfect Forward Secrecy, which is REQUIRED in [BSITLS], is supported by the TLS_ECDH(E)_* and TLS_DHE_* cipher suites, which should be supported. For performance reasons the elliptic curve (EC) encryption should be used. Since not all implementations support *DH* forms, RSA is still an option.

## 8. REFERENCES

[BSITLS] Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung. Bundesamt für Sicherheit in der Informationstechnik (BSI). Bonn, 08 Oktober 2013.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf
and
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

[ENISAAKSP] Algorithms, Key Sizes and Parameters Report 2013 recommendations version 1.0 – October 2013. ENISA.
http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report
and
Algorithms, Key Sizes and Parameters Report – 2014:
http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014

[TLSSP] Transport Layer Security (TLS) Parameters. Last Updated 2013-10-03. http://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-parameters-4

[RFC5246] T. Dierks et al. The Transport Layer Security (TLS) Protocol Version 1.2. IETF RFC 5246. August 2008.
http://tools.ietf.org/html/rfc5246

[CVE] Common Vulnerabilities and Exposures list, a starting point for https://cve.mitre.org/. CVE is a dictionary of publicly known information security vulnerabilities and exposures.

[CBP 2017-002-01-EX] Explanatory Notes CBP 2017-002/01

There are several internet sites with information on the subject. Sometimes the opinions are contradictory depending on the 'view', e.g. legacy/still safe or theoretical/practical or slow/fast protocols, etc.

Some links:

Study on cryptographic protocols:
http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/study-on-cryptographic-protocols

SSL LABS Server Test:
https://www.ssllabs.com/ssltest
Explanation

OWASP TLS:
https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

OTHERS:
http://cipherli.st

http://safecurves.cr.yp.to

http://weakdh.org/sysadmin.html

*************************