



## Proposal: Inclusion of Emerging Cryptographic Algorithms in SAML v2.x November 2005

**Attention:** OASIS Security Services Technical Committee (SSTC).

### 1. Background

Since 2003, the New Zealand Government has been advancing an All-of-government authentication programme. The first phase of the programme due to go live in November 2005 is the Government Log-on Service (GLS). The GLS is built on a centralised model, whereby Service Provider government agencies redirect customers to the GLS to authenticate themselves. The GLS, and additional services under development, use a range of standards, both international (such as SAML) and jurisdictional (such as the New Zealand Security of Information Technology – NZSIT – standards from Government Communications Security Bureau – GCSB – the New Zealand equivalent of the NSA in the USA).

The New Zealand All-of-government authentication programme has noted that the SAML v2.0 specifications (saml-sec-consider-2.0-os and saml-conformance-2.0-os) do not include reference to emerging cryptographic algorithms. The newer algorithms such as EC-DH are increasingly referenced in algorithm-dependent RFCs and jurisdiction-based standards.

In order to comply with NZSIT400, the New Zealand All-of-government authentication programme will be expected to move to using the newer cryptographic algorithms (where applicable) in conjunction with SAML implementations as vendor tools become available.

There is a (currently small, residual) concern that vendors supplying security applications and tool support to the programme are not being provided with uniform guidance from standards bodies.

### 2. Proposal

It is proposed that the OASIS SSTC considers including more comprehensive references, comments and conditions of use concerning the range of cryptographic algorithms (provided here in Table 1) in the current or next version of the OASIS standards, *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML)* [saml-sec-consider-2.0-os], and *Conformance Requirements for the OASIS Security assertion Markup Language (SAML)* [saml-conformance-2.0-os].

**Table 1: Cryptographic Algorithms**

<b>Cryptographic Algorithm</b>	<b>Algorithm Type</b>	<b>Reference</b>
Advanced Encryption Standard (AES)	Symmetric Encryption	FIPS 197
Secure Hashing Algorithm (SHA)	Hashing	FIPS 180-2
Elliptic Curve Diffie-Hellman (EC-DH) or Elliptic Curve Menezes-Qu-Vanstone (EC-MQV)	Key Establishment	NIST SP 800-56
Elliptic Curve Digital Signature Algorithm (EC-DSA)	Digital Signatures	FIPS 186-2

With regard to AES, it is further proposed that the SSTC considers including a reference to RFC3268 in Section 4.5 of saml-sec-consider-2.0-os and Section 4 of the saml-conformance-2.0-os.

With regard to SHA, it is further proposed that the SSTC considers including the specific rationale for the citation of FIPS 180-2, since it supersedes FIPS 180-1 and includes the additional algorithms SHA-256, SHA-384, and SHA-512.

### 3. Justifications

The justifications for this Proposal are described separately below.

#### AES

- The IETF TLS working group has developed AES ciphersuites for the TLS protocol [RFC3268] (with key sizes either 128-bit or 256-bit). Saml-sec-consider-2.0-os references TLS v1.0 [RFC2246] but not RFC3268.
- In New Zealand the Government Communications Security Bureau (GCSB) states that AES is the preferred symmetric encryption algorithm for IN-CONFIDENCE, SENSITIVE, and RESTRICTED information. Their recommendation is that the use of Triple DES should be phased out as soon as possible [NZSIT].
- The USA National Security Agency (NSA) has released a fact sheet NSA Suite B Cryptography [NSA], which includes AES (with key sizes of 128 and 256 bits) with the stated aim: 'to provide industry with a common set of cryptographic algorithms that they can use to create products that meet the needs of the widest range of USA Government needs'.
- The Overview section of RFC3268 also gives good arguments for moving to AES, such as efficiency, avoidance of IP claims, etc. while TLS v1.1 includes the AES ciphersuites of RFC3268 [TLSv1.1].
- The IP Security Protocol [IPSEC] working group has a number of RFCs covering AES with further AES developments underway.

#### SHA

- The status of SHA-1 is currently under consideration. Note that TLS v1.0 and TLS v1.1 [TLSv1.1] use SHA-1, but TLS v1.0 cites FIPS 180-1 whereas TLS v1.1 cites FIPS 180-2. It is proposed that TLS v1.2 addressing dependencies on the current hash functions (as well as for other cryptographic algorithms) [Rescorla].
- The National Institute of Standards and Technology (NIST) organised a cryptographic hash workshop for late October 2005, and have stated that they plan to phase out SHA-1 in favour of SHA-224, SHA-256, SHA-384 and SHA-512, see [Burr]. Transition issues relating to the use of hash algorithms (which also apply for general cryptosystems) are discussed in [Bellare].
- The TLS working group agenda at the sixty-fourth IETF meeting in November 2005 includes a discussion hash functions and TLS v1.2 (working group members will both attend and speak at the NIST cryptographic hash workshop mentioned above).
- In NZSIT400 GCSB states that SHA (FIPS 180-2) with a digest of at least 256 bits must be used for IN-CONFIDENCE, SENSITIVE, and RESTRICTED information [NZSIT].
- The NSA Suite B Cryptography hash functions are either SHA-256 or SHA-384 [NSA].

- Additional algorithm identifiers and encoding rules for Elliptic Curve (EC) with PKIX are being developed and include object identifiers for SHA-224, SHA-256, SHA-384, and SHA-512 for use with the EC algorithms [PKIX-EC].

## **Elliptic Curve Algorithms for Key Establishment and Digital Signatures**

It is recognised that Elliptic Curve (EC) algorithms for both key establishment and digital signatures have advantages over earlier algorithms in terms of efficiency and security [NSA-ECC]. NIST has recognised that the current 1024-bit security algorithms are sufficient for use until 2010, but this means that standards groups should move now to include appropriate algorithms for use beyond 2010.

The TC should consider including comments concerning these algorithms since:

- The TLS working group are developing EC ciphersuites for TLS, namely EC-DH and EC-DSA [TLS-EC].
- In NZSIT400 GCSB states that EC-DH or EC-MQV are the preferred key establishment algorithms while EC-DSA is the preferred digital signature algorithm for IN-CONFIDENCE, SENSITIVE and RESTRICTED information. Their recommendation is that the use of other algorithms (RSA, KEA, etc.) should be phased out [NZSIT].
- The NSA Suite B includes EC-DSA for digital signatures and EC-DH or EC-MQV for key establishment [NSA]. The NSA has also released a fact sheet 'outlining the case for moving to elliptic curves as a foundation for future Internet security' citing the reasons of better performance and higher security when compared to earlier public key algorithms [NSA-ECC].
- PKIX RFC 3279 includes object identifiers and encoding rules for EC-DSA [RFC 3279]. Additional algorithm identifiers and related encoding rules for EC use with PKIX are being developed covering EC-DSA, EC-DH and EC-MQV [PKIX-EC].

## **4. Contact**

Questions or comments in connection to this Proposal are welcome. They should be sent to All-of-government authentication programme, State Services Commission, PO Box 329, Wellington, New Zealand or email to: [authentication@ssc.govt.nz](mailto:authentication@ssc.govt.nz) copied to the authors; Dr. Marie Henderson ([marie.henderson@ssc.govt.nz](mailto:marie.henderson@ssc.govt.nz)) and Mr. Colin Wallis ([colin.wallis@ssc.govt.nz](mailto:colin.wallis@ssc.govt.nz)).

## 5. References

- [Bellovin] S. Bellovin and E. Rescorla, *Deploying New Hash Algorithms*, preprint. <<http://www.cs.columbia.edu/~smb/papers/new-hash.pdf>>
- [Burr] W. Burr, NIST brief comment on recent cryptanalytic attacks on SHA-1 and NIST plans. [www.csrc.nist.gov/pki/HashWorkshop/NIST%20Statement/Burr\\_Mar2005.html](http://www.csrc.nist.gov/pki/HashWorkshop/NIST%20Statement/Burr_Mar2005.html) (Accessed 19<sup>th</sup> October 2005.)
- [FIPS 180-2] National Institute of Standards and Technology, *Federal Information Processing Standards Publication 180-2: Secure Hash Standard*. August 1 2002. [www.itl.nist.gov/fipspubs/](http://www.itl.nist.gov/fipspubs/)
- [FIPS 186-2] National Institute of Standards and Technology, *Federal Information Processing Standards Publication 186: Digital Signature Standard*. January 27 2000. [www.itl.nist.gov/fipspubs/](http://www.itl.nist.gov/fipspubs/)
- [FIPS 197] National Institute of Standards and Technology, *Federal Information Processing Standards Publication 197: Advanced Encryption Standard*. November 26 2001. [www.itl.nist.gov/fipspubs/](http://www.itl.nist.gov/fipspubs/)
- [IPSEC] IP Security Protocol Charter. [www.ietf.org/html.charters/OLD/ipsec-charter.html](http://www.ietf.org/html.charters/OLD/ipsec-charter.html)
- [NIST SP 800-56] National Institute of Standards and Technology, *Draft- Special Publication 800-56: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. 6<sup>th</sup> July 2005. [csrc.nist.gov/publications/nistpubs/](http://csrc.nist.gov/publications/nistpubs/)
- [NSA] National Security Agency, *Fact Sheet - NSA Suite B Cryptography*, [www.nsa.gov/ia/](http://www.nsa.gov/ia/) (Accessed 19<sup>th</sup> October 2005.)
- [NSA-ECC] National Security Agency, *Fact sheet – The Case for Elliptic Curve Cryptography*, [www.nsa.gov/ia/](http://www.nsa.gov/ia/) (Accessed 19<sup>th</sup> October 2005.)
- [NZSIT] Government Communications Security Bureau, *New Zealand Security of Information Technology 400*. October 2005. [www.gcsb.govt.nz](http://www.gcsb.govt.nz)
- [PKIX-EC] PKIX working group, *Internet draft – Additional Algorithms and Identifiers for use of Elliptic Curve Cryptography with PKIX*, March 31 2005. [www.ietf.org](http://www.ietf.org).
- [RFC2246] T. Dierks and C. Allen. *The TLS Protocol Version 1.0*. IETF RFC 2246, January 1999. [www.ietf.org](http://www.ietf.org)
- [RFC3268] P. Chown. *AES Ciphersuites for TLS*, IETF RFC 3268, June 2002. [www.ietf.org](http://www.ietf.org)
- [Rescorla] E. Rescorla, *[TLS] Proposed TLS WG recharter*, 17<sup>th</sup> November 2005. Posting to TLS mailing list. <http://www.imc.org/ietf-tls/mail-archive/msg04809.html>
- [SPC-SAML] F. Hirsch et al. *Security and Privacy Considerations for OASIS Security Assertion Markup Language (SAML) V2.0*. 15<sup>th</sup> March 2005. [www.oasis-open.org/committees/security](http://www.oasis-open.org/committees/security)
- [TLS-EC] V. Gupta et al. *Internet-draft: ECC Cipher Suites for TLS*, September 2005 (Expires March 20, 2006). [www.ietf.org](http://www.ietf.org)
- [TLSv1.1] T. Dierks and E. Rescorla. *Internet-draft: The TLS Protocol Version 1.1*, June 2005 (Expires December 2005). [www.ietf.org](http://www.ietf.org)