Network Working Group L. Howard
Internet-Draft PADL
Intended status: Experimental April 6, 2020
Expires: October 8, 2020

# A Simple Anonymous GSS-API Mechanism
## draft-howard-gss-sanon-02

Abstract

This document defines protocols, procedures and conventions for a Generic Security Service Application Program Interface (GSS-API) security mechanism that provides key agreement without authentication of either party.

Table of Contents

1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . 2
1.1. Authentication . . . . . . . . . . . . . . . . . . . . . . 3
1.2. Application Services . . . . . . . . . . . . . . . . . . . 3
2. Requirements notation . . . . . . . . . . . . . . . . . . . . 3
3. Discovery and Negotiation . . . . . . . . . . . . . . . . . . 3
4. Naming . . . . . . . . . . . . . . . . . . . . . . . . . . . 4
4.1. GSS Name Types . . . . . . . . . . . . . . . . . . . . . . 4
4.1.1. GSS_C_NT_USER_NAME . . . . . . . . . . . . . . . . . . 4
4.1.2. GSS_C_NT_HOSTBASED_SERVICE . . . . . . . . . . . . . . 4
4.1.3. GSS_C_NT_DOMAINBASED_SERVICE . . . . . . . . . . . . . 4
4.1.4. GSS_C_NT_ANONYMOUS . . . . . . . . . . . . . . . . . . 4
4.2. Canonicalization . . . . . . . . . . . . . . . . . . . . . 4
4.3. Mechanism Selection Hints . . . . . . . . . . . . . . . . . 5
5. Mechanism Attributes . . . . . . . . . . . . . . . . . . . . 5
6. Definitions and Token Formats . . . . . . . . . . . . . . . . 6
6.1. Context Establishment Tokens . . . . . . . . . . . . . . . 6
6.1.1. Initial context token . . . . . . . . . . . . . . . . . 6
6.1.2. Acceptor context token . . . . . . . . . . . . . . . . 6
6.1.3. Initiator context completion . . . . . . . . . . . . . 7
6.2. Per-Message Tokens . . . . . . . . . . . . . . . . . . . . 7
6.3. Context Deletion Tokens . . . . . . . . . . . . . . . . . . 7
6.4. Exported Name Tokens . . . . . . . . . . . . . . . . . . . 7
7. Key derivation . . . . . . . . . . . . . . . . . . . . . . . 7
8. Pseudo-Random Function . . . . . . . . . . . . . . . . . . . 8
9. NegoEx . . . . . . . . . . . . . . . . . . . . . . . . . . . 8
10. Test Vectors . . . . . . . . . . . . . . . . . . . . . . . . 9
11. Security Considerations . . . . . . . . . . . . . . . . . . . 9
12. IANA Considerations . . . . . . . . . . . . . . . . . . . . . 9
13. Acknowledgements . . . . . . . . . . . . . . . . . . . . . . 10
14. Normative References . . . . . . . . . . . . . . . . . . . . 10
Author's Address . . . . . . . . . . . . . . . . . . . . . . . . 11

## 1. Introduction

The Generic Security Service Application Program Interface (GSS-API) [RFC2743] provides a framework for authentication and message protection services through a common programming interface.

The Simple Anonymous mechanism described in this document (hereafter SAnon) is a simple protocol based on the X25519 elliptic curve Diffie-Hellman (ECDH) key agreement scheme defined in [RFC7748]. No authentication of initiator or acceptor is provided. A potential use of SAnon is to provide a degree of privacy when bootstrapping unkeyed entities.

### 1.1. Authentication

The GSS-API protocol involves a client, known as the initiator, sending an initial security context token of a chosen GSS-API security mechanism to a peer, known as the acceptor. The two peers subsequently exchange, synchronously, as many security context tokens as necessary to complete the authentication or fail. The specific number of context tokens exchanged varies by security mechanism: in the case of the SAnon mechanism, it is two (i.e. a single round trip). Once authentication is complete, the initiator and acceptor share a security context which can be used for integrity or confidentiality, protecting subsequent application messages.

### 1.2. Application Services

GSS-API provides a number of a services to the calling application:

GSS_Wrap() integrity and optional confidentiality for a message

GSS_GetMIC() integrity for a message sent separately

GSS_Pseudo_random() shared key derivation (e.g., for keying external confidentiality and integrity layers)

These services are used with security contexts having a shared session key to protect application-layer messages.

## 2. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

## 3. Discovery and Negotiation

The means of discovering GSS-API peers and their supported mechanisms is out of this specification's scope. Mechanisms are typically explicitly selected by the initiator, or selected from a set of common mechanisms using the Simple and Protected Negotiation mechanism (SPNEGO) defined in [RFC4178]. An initiator that that supports the [I-D.zhu-negoex] protocol MUST negotiate SAnon using NegoEx rather than using SPNEGO directly. Initiators that do not support NegoEx MAY negotiate SAnon directly under SPNEGO.

To avoid multiple negotiation layers and implementation complexity, this specification is deliberately not crypto-agile. A future variant using a different key exchange algorithm would be assigned a different mechanism OID and authentication scheme identifier.

If anonymity is not desired then SAnon MUST NOT be used. Either party can test for the presence of GSS_C_ANON_FLAG to check if anonymous authentication was performed.

## 4. Naming

The GSS-API provides a rich security principal naming model. At its most basic the query forms of names consist of a user-entered/ displayable string and a "name-type". Name-types are constants with names prefixed with "GSS_C_NT_" in the GSS-API.

### 4.1. GSS Name Types

#### 4.1.1. GSS_C_NT_USER_NAME

This name type is supported when the input name string is the well known anonymous name string, WELLKNOWN/ANONYMOUS@WELLKNOWN:ANONYMOUS. In all other cases, importing the name MUST fail.

#### 4.1.2. GSS_C_NT_HOSTBASED_SERVICE

This name type identifies a host-based service and is generally used by acceptors. To allow existing applications to work unmodified with SAnon, it is useful to allow anonymous acceptor credentials to be acquired regardless of the service name. (It follows from SAnon not performing mutual authentication that the acceptor identity is meaningless.) When importing a name of this type the name string SHOULD be ignored.

#### 4.1.3. GSS_C_NT_DOMAINBASED_SERVICE

The [RFC5179] name type, along with all other acceptor name types, are treated identically to GSS_C_NT_HOSTBASED_SERVICE.

#### 4.1.4. GSS_C_NT_ANONYMOUS

When importing a name of this type the name string MUST be ignored. Functions that return a name type to the caller MUST always return this name type. The display form is the well known anonymous name string, WELLKNOWN/ANONYMOUS@WELLKNOWN:ANONYMOUS. This is always the name observed by a SAnon peer.

### 4.2. Canonicalization

The SAnon GSS-API mechanism has a single anonymous identity, the well known anonymous name. The canonical form is the well known anonymous name string with the GSS_C_NT_ANONYMOUS name type.

### 4.3. Mechanism Selection Hints

Many deployed applications do not have explicit support for anonymous authentication. To ease deployment, we recommend allowing anonymous authentication to be requested by the initiator acquiring a credential with a well known anonymous name. This may allow the end-user to request anonymous authentication directly, without requiring the application be modified to support GSS_C_ANON_FLAG. The well known anonymous name has the same display form as in Kerberos [RFC8062], allowing acceptors to perform name-based authorization in a mechanism-agnostic manner.

This approach may, however, disadvantage applications that wish to use GSS_C_ANON_FLAG to select anonymous authentication, as importing a non-anonymous initiator name would fail with this approach. We consider this an acceptable compromise given the limited deployment of GSS_C_ANON_FLAG in existing implementations.

## 5. Mechanism Attributes

The [RFC5587] mechanism attributes for this mechanism are:

GSS_C_MA_MECH_CONCRETE

GSS_C_MA_ITOK_FRAMED

GSS_C_MA_AUTH_INIT_ANON

GSS_C_MA_AUTH_TARG_ANON

GSS_C_MA_INTEG_PROT

GSS_C_MA_CONF_PROT

GSS_C_MA_MIC

GSS_C_MA_WRAP

GSS_C_MA_REPLAY_DET

GSS_C_MA_OOS_DET

GSS_C_MA_CBINDINGS

GSS_C_MA_PFS

GSS_C_MA_CTX_TRANS

## 6. Definitions and Token Formats

### 6.1. Context Establishment Tokens

#### 6.1.1. Initial context token

The initial context token is framed per Section 1 of [RFC2743]:

```
GSS-API DEFINITIONS ::=
     BEGIN

     MechType ::= OBJECT IDENTIFIER
     -- representing SAnon mechanism
     GSSAPI-Token ::=
     [APPLICATION 0] IMPLICIT SEQUENCE {
         thisMech MechType,
         innerToken ANY DEFINED BY thisMech
             -- 32 byte initiator public key
     }
     END
```

On the first call to GSS_Init_sec_context(), the mechanism checks for one of the following:

The caller set anon_req_flag (GSS_C_ANON_FLAG); or

The claimant_cred_handle identity is the well known anonymous name; or

The claimant_cred_handle is the default credential and targ_name an anonymous name.

If none of the above are the case, the call MUST fail with GSS_S_UNAVAILABLE.

If proceeding, the initiator generates a fresh secret and public key pair per Section 6.1 of [RFC7748] and returns GSS_S_CONTINUE_NEEDED indicating that a subsequent context token from the acceptor is expected. The innerToken field of the output_token contains the initiator's 32 byte public key.

#### 6.1.2. Acceptor context token

Upon receiving a context token from the initiator, the acceptor validates that the token is well formed and contains a public key of the requisite length. The acceptor generates a fresh secret and public key pair. A session key is computed as specified in Section 7.

The acceptor constructs an output_token by concatenating its public key with the token emitted by calling GSS_GetMIC() with the default QOP and zero-length octet string. The output token is sent to the initiator without additional framing.

The acceptor then returns GSS_S_COMPLETE, setting src_name to the well known anonymous name. The reply_det_state (GSS_C_REPLAY_FLAG), sequence_state (GSS_C_SEQUENCE_FLAG), conf_avail (GSS_C_CONF_FLAG), integ_avail (GSS_C_INTEG_FLAG) and anon_state (GSS_C_ANON_FLAG) security context flags are set to TRUE. The context is ready to use.

#### 6.1.3. Initiator context completion

Upon receiving the acceptor context token and verifying it is well formed, the initiator extracts the acceptor's public key (being the first 32 bytes of the input token) and computes the session key per Section 7. The initiator then calls GSS_VerifyMIC() with the default QOP and zero-length octet string. If successful, the initiator returns GSS_S_COMPLETE to the caller, to indicate the initiator is authenticated and the context is ready for use. No output token is emitted. Security context flags are set as for the acceptor context.

### 6.2. Per-Message Tokens

The per-message tokens definitions are imported from [RFC4121] Section 4.2. The base key used to derive specific keys for signing and sealing messages is the session key defined in Section 7. The [RFC3961] encryption and checksum algorithms use the aes128-cts-hmac-sha256-128 encryption type defined in [RFC8009]. The AcceptorSubkey flag as defined in [RFC4121] Section 4.2.2 MUST be set.

### 6.3. Context Deletion Tokens

Context deletion tokens are empty in this mechanism. The behavior of GSS_Delete_sec_context() [RFC2743] is as specified in [RFC4121] Section 4.3.

### 6.4. Exported Name Tokens

The exported name token format for the SAnon GSS-API mechanism is the same as the display form, plus the standard exported name token format header mandated by the GSS-API [RFC2743].

## 7. Key derivation

The ECDH shared secret k is computed by calling the X25519 function with the local secret key and the peer's public key, as specified in Section 6.1 of [RFC7748]. The context session key (K1) is computed

using a key derivation function from Section 5.1 of [SP800-108] with HMAC as the PRF:

```
K1 = HMAC-SHA-256(key, 0x00000001 | label | 0x00 | context | k)
```

where:

k              the X25519 shared secret computed above

0x00000001     the iteration count from Section 5.1 of [SP800-108]

label          the string "sanon-x25519" (without quotation marks)

context        the concatenation of the initiator and acceptor public keys, along with the channel binding application data (if present), in that order

The inclusion of channel bindings in the key derivation function means that the acceptor cannot ignore initiator channel bindings; this differs from some other mechanisms.

This session key is equivalent to the acceptor-asserted subkey defined in [RFC4121] Section 2 and is used as the base key for generating keys for per-message tokens and the GSS-API PRF.

The session key encryption type is aes128-cts-hmac-sha256-128 as defined in [RFC8009].  The [RFC3961] algorithm protocol parameters are as given in [RFC8009] Section 5.

## 8. Pseudo-Random Function

The [RFC4401] GSS-API pseudo-random function for this mechanism imports the definitions from [RFC8009], using the context session key as the base key for both GSS_C_PRF_KEY_FULL and GSS_C_PRF_KEY_PARTIAL usages.

## 9. NegoEx

The NegoEx authentication scheme identifier for this mechanism is DEE384FF-1086-4E86-BE78-B94170BFD376.

The initiator and acceptor keys for NegoEx checksum generation and verification are derived using the PRF from the previous section, with the input data "sanon-x25519-initiator-negoex-key" and "sanon-x25519-acceptor-negoex-key" respectively (without quotation marks).

No NegoEx metadata is specified.  Any metadata present MUST be ignored.

## 10. Test Vectors

```
initiator secret key  69 df cc 04 2b 7a 33 f8 1a 43 fb f0 33 0a b5 3f
                      bc 20 e6 c1 4f f8 26 ce 6a 4d bc 8c 6e e4 2b a9

initiator public key  d2 1e 3e 58 60 b0 16 6c d1 cb 38 1a aa 89 62 93
                      07 13 ae e1 76 86 93 10 46 57 a7 a1 9c 1d 76 2e

initiator token       60 2c 06 0a 2b 06 01 04 01 a9 4a 1a 01 6e d2 1e
                      3e 58 60 b0 16 6c d1 cb 38 1a aa 89 62 93 07 13
                      ae e1 76 86 93 10 46 57 a7 a1 9c 1d 76 2e

acceptor secret key   3e 4f e6 5b ea 85 94 3b 5a a2 b7 83 f6 26 84 1a
                      10 39 d5 d3 6d af 85 aa a1 6f 12 97 57 99 6c ff

acceptor public key   a8 32 14 9d 58 33 13 ce 1c 55 7b 2b d1 8a e7 a5
                      59 8c a6 4b 02 20 83 5e 16 be 09 ca 2f 90 60 31

context session key   af f1 8d b7 45 c6 27 cd a8 da d4 9b d7 e7 01 25

acceptor token        a8 32 14 9d 58 33 13 ce 1c 55 7b 2b d1 8a e7 a5
                      59 8c a6 4b 02 20 83 5e 16 be 09 ca 2f 90 60 31
                      04 04 05 ff ff ff ff ff 00 00 00 00 00 00 00 00
                      45 02 7b a8 15 1c 33 05 22 bb c4 36 84 d2 e1 8c
```

## 11. Security Considerations

This document defines a GSS-API security mechanism, and therefore deals in security and has security considerations text embedded throughout. This section only addresses security considerations associated with the SAnon mechanism described in this document. It does not address security considerations associated with the GSS-API itself.

This mechanism provides only for key agreement. It does not authenticate or identify either party. It MUST not be selected if either party requires identification of its peer.

## 12. IANA Considerations

IANA is requested to assign an OID for this GSS-API mechanism in the SMI numbers registry, with the prefix of iso.org.dod.internet.security.mechanisms (1.3.6.1.5.5) and to reference this specification in the registry.

## 13. Acknowledgements

AuriStor, Inc funded the design of this protocol, along with an implementation for the Heimdal GSS-API library.

Jeffrey Altman, Greg Hudson, Simon Josefsson, and Nicolas Williams provided valuable feedback on this document.

## 14. Normative References

[I-D.zhu-negoex]
Short, M., Zhu, L., Damour, K., and D. McPherson, "SPNEGO Extended Negotiation (NEGOEX) Security Mechanism", draft-zhu-negoex-04 (work in progress), January 2011.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2743] Linn, J., "Generic Security Service Application Program Interface Version 2, Update 1", RFC 2743, DOI 10.17487/RFC2743, January 2000, <https://www.rfc-editor.org/info/rfc2743>.

[RFC3961] Raeburn, K., "Encryption and Checksum Specifications for Kerberos 5", RFC 3961, DOI 10.17487/RFC3961, February 2005, <https://www.rfc-editor.org/info/rfc3961>.

[RFC4121] Zhu, L., Jaganathan, K., and S. Hartman, "The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2", RFC 4121, DOI 10.17487/RFC4121, July 2005, <https://www.rfc-editor.org/info/rfc4121>.

[RFC4178] Zhu, L., Leach, P., Jaganathan, K., and W. Ingersoll, "The Simple and Protected Generic Security Service Application Program Interface (GSS-API) Negotiation Mechanism", RFC 4178, DOI 10.17487/RFC4178, October 2005, <https://www.rfc-editor.org/info/rfc4178>.

[RFC4401] Williams, N., "A Pseudo-Random Function (PRF) API Extension for the Generic Security Service Application Program Interface (GSS-API)", RFC 4401, DOI 10.17487/RFC4401, February 2006, <https://www.rfc-editor.org/info/rfc4401>.

[RFC5179] Williams, N., "Generic Security Service Application Program Interface (GSS-API) Domain-Based Service Names Mapping for the Kerberos V GSS Mechanism", RFC 5179, DOI 10.17487/RFC5179, May 2008, <https://www.rfc-editor.org/info/rfc5179>.

[RFC5587] Williams, N., "Extended Generic Security Service Mechanism Inquiry APIs", RFC 5587, DOI 10.17487/RFC5587, July 2009, <https://www.rfc-editor.org/info/rfc5587>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/info/rfc7748>.

[RFC8009] Jenkins, M., Peck, M., and K. Burgin, "AES Encryption with HMAC-SHA2 for Kerberos 5", RFC 8009, DOI 10.17487/RFC8009, October 2016, <https://www.rfc-editor.org/info/rfc8009>.

[RFC8062] Zhu, L., Leach, P., Hartman, S., and S. Emery, Ed., "Anonymity Support for Kerberos", RFC 8062, DOI 10.17487/RFC8062, February 2017, <https://www.rfc-editor.org/info/rfc8062>.

[SP800-108] Chen, L., "Recommendation for Key Derivation Using Pseudorandom Functions (Revised)", October 2009.

## Author's Address

Luke Howard
PADL Software Pty Ltd
PO Box 59
Central Park, VIC 3145
Australia

Email: lukeh@padl.com