

Simple Authentication and Security Layer (SASL)

Status of this Memo

This document is an Internet Draft and is in full conformance with all provisions of [Section 10 of RFC 2026](#).

Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its Areas, and its Working Groups. Note that other groups may also distribute working documents as Internet Drafts. Internet Drafts are draft documents valid for a maximum of six months. Internet Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet Drafts as reference material or to cite them other than as ``work in progress''.

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

A revised version of this draft document will be submitted to the RFC editor as a Draft Standard for the Internet Community. Discussion and suggestions for improvement are requested. Distribution of this draft is unlimited.

1. Abstract

SASL provides a method for adding authentication support with an optional security layer to connection-based protocols. It also describes a structure for authentication mechanisms. The result is an abstraction layer between protocols and authentication mechanisms such that any SASL-compatible authentication mechanism can be used with any SASL-compatible protocol.

This document describes how a SASL authentication mechanism is structured, how a protocol adds support for SASL, defines the protocol for carrying a security layer over a connection, and defines the EXTERNAL SASL authentication mechanism.

2. Organization of this document

2.1. How to read this document

This document is written to serve two different audiences, protocol designers using this specification to support authentication in their protocol, and implementors of clients or servers for those protocols using this specification.

The sections "Overview", "Authentication Mechanisms", "Protocol Profile Requirements", "Specific Issues", and "Security Considerations" cover issues that protocol designers need to understand and address in profiling this specification for use in a specific protocol.

Implementors of a protocol using this specification need the protocol-specific profiling information in addition to the information in this document.

2.2. Conventions used in this document

In examples, "C:" and "S:" indicate lines sent by the client and server respectively.

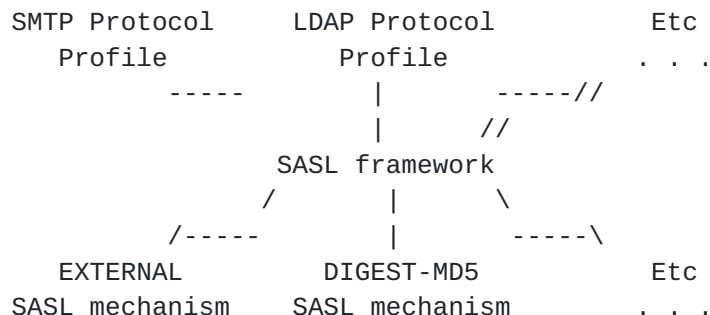
The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as defined in "Key words for use in RFCs to Indicate Requirement Levels" [[KEYWORDS](#)].

3. Overview

The Simple Authentication and Security Layer (SASL) is a method for adding authentication support to connection-based protocols.

The SASL specification has three layers, as indicated in the diagram

below. At the top, a protocol definition using SASL specifies a profile, including a command for identifying and authenticating a user to a server and for optionally negotiating a security layer for subsequent protocol interactions. At the bottom, a SASL mechanism definition specifies an authentication mechanism. The SASL framework, specified by this document, constrains the behavior of protocol profiles and mechanisms, separating protocol from mechanism and defining how they interact.



This separation between the definition of protocols and the definition of authentication mechanisms is crucial. It permits an authentication mechanism to be defined once, making it usable by any SASL protocol profiles. In many implementations, the same SASL mechanism code is used for multiple protocols.

4. Authentication mechanisms

SASL mechanisms are named by strings, from 1 to 20 characters in length, consisting of upper-case letters, digits, hyphens, and/or underscores. SASL mechanism names must be registered with the IANA. IETF Standards Track documents may override this registration requirement by reserving a portion of the SASL mechanism namespace for their own use; the GSSAPI mechanism specification [SASL-GSSAPI] does this. Procedures for registering new SASL mechanisms are given in the section "Registration procedures".

The "sasl-mech" rule below defines the syntax of a SASL mechanism name. This uses the augmented Backus-Naur Form (BNF) notation as specified in [ABNF] and the ABNF core rules as specified in [Appendix A](#) of the ABNF specification [ABNF].

```

sasl-mech    = 1*20mech-char
mech-char    = %x41-5A / DIGIT / "-" / "_"
              ; mech names restricted to uppercase letters,
              ; digits, "-" and "_"
  
```


4.1. Authentication protocol exchange

A SASL mechanism is responsible for conducting an authentication protocol exchange. This consists of a series of server challenges and client responses, the contents of which are specific to and defined by the mechanism. To the protocol, the challenges and responses are opaque binary tokens of arbitrary length. The protocol's profile then specifies how these binary tokens are then encoded for transfer over the connection.

After receiving an authentication command or any client response, a server mechanism may issue a challenge, indicate failure, or indicate completion. The server mechanism MAY return additional data with a completion indication. The protocol's profile specifies how each of these is then represented over the connection.

After receiving a challenge, a client mechanism may issue a response or abort the exchange. The protocol's profile specifies how each of these is then represented over the connection.

During the authentication protocol exchange, the mechanism performs authentication, transmits an authorization identity (frequently known as a userid) from the client to server, and negotiates the use of a mechanism-specific security layer. If the use of a security layer is agreed upon, then the mechanism must also define or negotiate the maximum security layer buffer size that each side is able to receive.

4.2. Authorization identities and proxy authentication

An authorization identity is a string of zero or more ISO 10646 [[ISO-10646](#)] coded characters. The NUL (U+0000) character is not permitted in authorization identities. The meaning of an authorization identity of the empty string (zero length) is defined below in this section. The authorization identity is used by the server as the primary identity for making access policy decisions.

The character encoding scheme used for transmitting an authorization identity over protocol is specified in each authentication mechanism (with the authentication mechanism's blob being further restricted/encoded by the protocol profile). Per IETF character set policy [[CHARSET-POLICY](#)], authentication mechanisms SHOULD encode these and other strings in UTF-8 [[UTF-8](#)]. While some legacy mechanisms are incapable of transmitting an authorization identity other than the empty string, newly defined mechanisms are expected to be capable of carrying the entire Unicode repertoire (with the exception of the NUL character). An authorization identity of the empty string and an absent authorization identity MUST be treated as equivalent. However, mechanisms SHOULD NOT allow both (i.e. if an

authorization identity is allowed to be absent, but one is transferred, it SHOULD NOT be an empty string).

The identity derived from the client's authentication credentials is known as the "authentication identity". With any mechanism, transmitting an authorization identity of the empty string directs the server to derive an authorization identity from the client's authentication identity.

If the authorization identity transmitted during the authentication protocol exchange is not the empty string, this is typically referred to as "proxy authentication". This feature permits agents such as proxy servers to authenticate using their own credentials, yet request the access privileges of the identity for which they are proxying.

The server makes an implementation defined policy decision as to whether the authentication identity is permitted to have the access privileges of the authorization identity and whether the authorization identity is permitted to receive service. If it is not, the server indicates failure of the authentication protocol exchange.

As a client might not have the same information as the server, clients SHOULD NOT themselves try to derive authorization identities from authentication identities when clients could instead transmit an authorization identity of the empty string.

The server SHOULD verify the correctness of a received authorization identity. Profiles whose authorization identities are simple user names (e.g. IMAP [[RFC 3501](#)]) are encouraged to employ [[SASLPrep](#)] profile [[SASLPrep](#)] of the "stringprep" algorithm [[StringPrep](#)] to prepare these names for matching. If the preparation of the authorization identity fails or results in an empty string, the server MUST fail the authentication exchange. The only exception to this rule is when the received authorization identity is already the empty string.

[4.3.](#) Security layers

If use of a security layer is negotiated by the authentication protocol exchange, the security layer is applied to all subsequent data sent over the connection. The security layer takes effect immediately following the last response of the authentication exchange for data sent by the client and the completion indication for data sent by the server.

Once the security layer is in effect, the protocol stream is processed by the security layer into buffers of security encoded data. Each buffer of security encoded data is transferred over the connection as a stream of octets prepended with a four octet field in network byte order that represents the length of the following buffer. The length of the security encoded data buffer MUST be no larger than the maximum size that was either defined in the mechanism specification or negotiated by the other side during the authentication protocol exchange. Upon the receipt of a data buffer which is larger than the defined/negotiated maximal buffer size, the receiver SHOULD close the connection. This might be a sign of an attack or a buggy implementation.

4.4. Character string issues

Per IETF character set policy [[CHARSET-POLICY](#)], authentication mechanisms SHOULD encode character strings in UTF-8 [[UTF-8](#)]. In order to avoid noninteroperability due to differing normalizations, when a mechanism specifies that a string authentication identity or password used as input to a cryptographic function (or used for comparison) it SHOULD specify that the string first be prepared using the "SASLPrep" profile [[SASLPrep](#)], of the "stringprep" algorithm [StringPrep]. This should be done by both the client (upon getting user input or retrieving a value from configuration) and by the server (upon receiving the value from the client). If preparation fails or results in an empty string, the client/server SHALL fail the authentication exchange.

5. Protocol profile requirements

In order to use this specification, a protocol definition MUST supply the following information:

A service name, to be selected from the IANA registry of "service" elements for the GSSAPI host-based service name form. [[GSSAPI](#)] This service name is made available to the authentication mechanism.

The registry is available at the URL

"<http://www.iana.org/assignments/gssapi-service-names>" A definition of the command to initiate the authentication protocol exchange. This command must have as a parameter the name of the mechanism being selected by the client.

The command SHOULD have an optional parameter giving an initial response. This optional parameter allows the client to avoid a round trip when using a mechanism which is defined to have the client send data first. When this initial response is sent by the client and the

selected mechanism is defined to have the server start with an initial challenge, the command fails. See [section 6.1](#) of this document for further information.

A definition of the method by which the authentication protocol exchange is carried out, including how the challenges and responses are encoded, how the server indicates completion or failure of the exchange, how the client aborts an exchange, and how the exchange method interacts with any line length limits in the protocol.

The command SHOULD have a method for the server to include an optional challenge with a success notification. This allows the server to avoid a round trip when using a mechanism which is defined to have the server send additional data along with the indication of successful completion. See [section 6.2](#) of this document for further information.

In addition, a protocol profile SHOULD specify a mechanism through which a client may obtain the names of the SASL mechanisms available to it. This is typically done through the protocol's extensions or capabilities mechanism.

Identification of the octet where any negotiated security layer starts to take effect, in both directions.

If both TLS and SASL security layer are allowed to be negotiated by the protocol, the protocol profile MUST define in which order they are applied to a cleartext data sent over the connection.

A protocol profile MAY further refine the definition of an authorization identity by adding additional syntactic restrictions and protocol-specific semantics. A protocol profile MUST specify the form of the authorization identity (as it is protocol specific, as opposed to the authentication identity which is mechanism specific) and how authorization identities are to be compared. Profiles whose authorization identities are simple user names (e.g. IMAP [\[RFC 3501\]](#)) are encouraged to employ [\[SASLPrep\]](#) profile [\[SASLPrep\]](#) of the "stringprep" algorithm [\[StringPrep\]](#) to prepare these names for matching.

Certain SASL mechanisms, e.g. DIGEST-MD5 [\[SASL-DIGEST\]](#), use a concept of realm. Conceptually, realm is the name of a collection of user's accounts. Realms allow the protected resources on a server to be partitioned into a set of protection spaces, each with its own authentication mechanisms and/or authorization database. For example, a proxy/frontend can use different realms for different servers/backends it represents. The realm value is a case-insensitive string, generally assigned by the origin server, which

may have additional semantics specific to the authentication mechanism.

A protocol profile SHOULD provide a guidance how realms are to be constructed and used in the protocol and MAY further restrict its syntax and protocol-specific semantics.

A protocol profile SHOULD NOT attempt to amend the definition of mechanisms or make mechanism-specific encodings. This breaks the separation between protocol and mechanism that is fundamental to the design of SASL.

6. Specific issues

6.1. Client sends data first

Some mechanisms specify that the first data sent in the authentication protocol exchange is from the client to the server.

If a protocol's profile permits the command which initiates an authentication protocol exchange to contain an initial client response, this parameter SHOULD be used with such mechanisms.

If the initial client response parameter is not given, or if a protocol's profile does not permit the command which initiates an authentication protocol exchange to contain an initial client response, then the server issues a challenge with no data. The client's response to this challenge is then used as the initial client response. (The server then proceeds to send the next challenge, indicates completion, or indicates failure.)

6.2. Server returns success with additional data

Some mechanisms may specify that additional data be sent to the client along with an indication of successful completion of the exchange. This data would, for example, authenticate the server to the client.

If a protocol's profile does not permit this additional data to be returned with a success indication, then the server issues the data as a server challenge, without an indication of successful completion. The client then responds with no data. After receiving this empty response, the server then indicates successful completion (with no additional data).

Client implementors should be aware of an additional failure case that might occur when the profile supports sending the additional data with success. Imagine that an active attacker is trying to

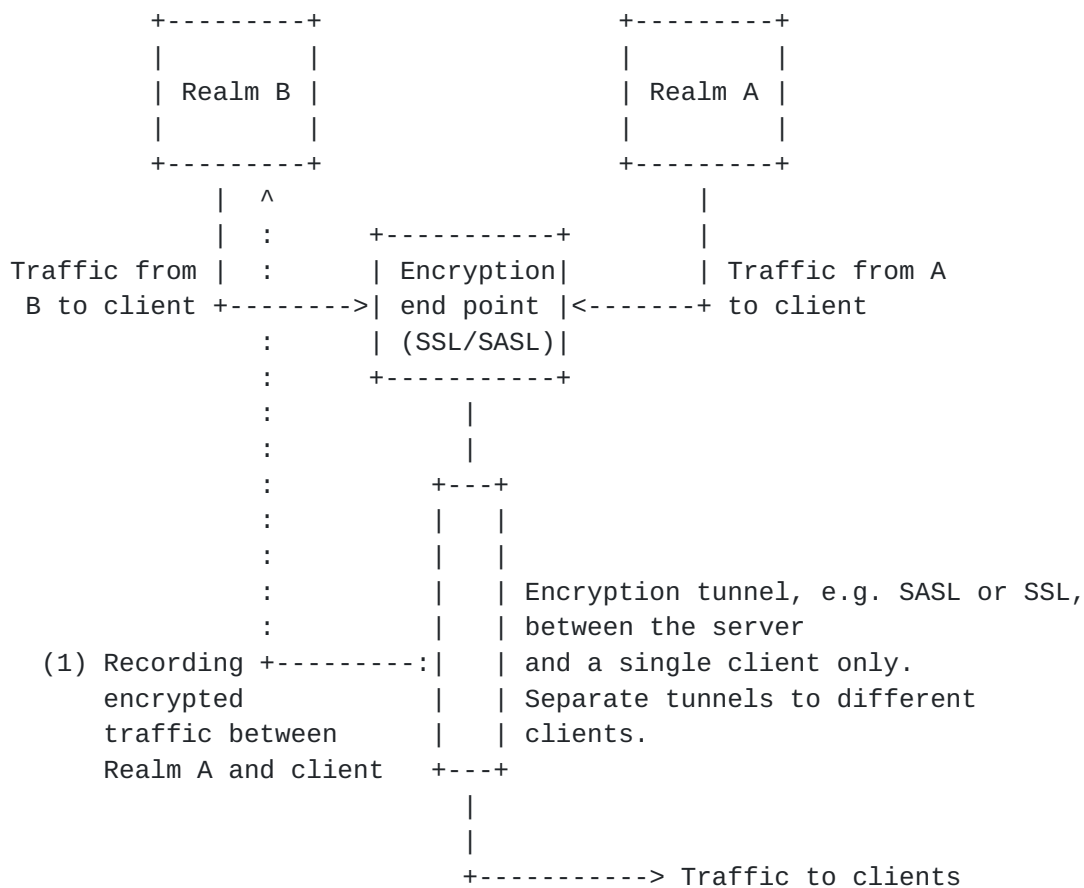
impersonate the server and sends a faked data, that should be used to authenticate the server to the client, with success. (A similar situation can happen when either the server and/or the client has a bug and they calculate different responses). After checking the data the client will think that the authentication exchange has failed, however the server will think that the authentication exchange has completed successfully. At this point the client can't abort the authentication exchange, it SHOULD close the connection instead. However, if the profile didn't support sending of additional data with success, the client could have aborted the exchange at the very last step of the authentication exchange.

6.3. Multiple authentications

Unless otherwise stated by the protocol's profile, only one successful SASL negotiation may occur in a protocol session. In this case, once an authentication protocol exchange has successfully completed, further attempts to initiate an authentication protocol exchange fail.

In the case that a profile explicitly permits multiple successful SASL negotiations to occur, then in no case may multiple security layers be simultaneously in effect. If a security layer is in effect and a subsequent SASL negotiation selects a second security layer, then the second security layer replaces the first. If a security layer is in effect and a subsequent SASL negotiation selects no security layer, the original security layer must be removed. The next paragraph explains why this is important.

Below the term "realm" has the meaning as defined in the [section 5](#). A security layer that remains in effect when a client, which already has authenticated and established the security layer with "Realm A", authenticates to "Realm B", without negotiating a new security layer, enables "Realm B" to make guesses about previously observed ciphertext using the server's SASL engine as an oracle. "Realm B" may observe how known cleartext is encrypted.



7. The EXTERNAL mechanism

```
The mechanism name associated with external authentication is
"EXTERNAL".
```

The client sends an initial response with the UTF-8 encoding of the authorization identity. The form of the authorization identity is further restricted by the application-level protocol's SASL profile.

The server uses information, external to SASL, to determine whether the client is authorized to authenticate as the authorization identity. If the client is so authorized, the server indicates successful completion of the authentication exchange; otherwise the server indicates failure.

The system providing this external information may be, for example, IPsec or TLS.

If the client sends the empty string as the authorization identity (thus requesting the authorization identity be derived from the client's authentication credentials), the authorization identity is to be derived from authentication credentials which exist in the

system which is providing the external authentication.

7.1. Formal syntax

The following syntax specification uses the augmented Backus-Naur Form (BNF) notation as specified in [\[ABNF\]](#). This uses the ABNF core rules as specified in [Appendix A](#) of the ABNF specification [\[ABNF\]](#). Non-terminals referenced but not defined below are as defined by [\[UTF-8\]](#).

The "initial-response" rule below defines the initial response sent from client to server.

```
initial-response = *( UTF8-char-no-null )
```

```
UTF8-char-no-null = UTF8-1-no-null / UTF8-2 / UTF8-3 / UTF8-4
```

```
UTF8-1-no-null    = %x01-7F
```

7.2. Example

The following is an example of an EXTERNAL authentication in the SMTP protocol [\[SMTP-AUTH\]](#). In this example, the client is proxy authenticating, sending the authorization id "fred". The server has determined the client's identity through IPsec and has a security policy that permits that identity to proxy authenticate as any other identity.

To the protocol profile, the four octet sequence "fred" is an opaque binary blob. The SASL protocol profile for SMTP specifies that server challenges and client responses are encoded in BASE64; the BASE64 encoding of "fred" is "ZnJlZA==".

```
S: 220 smtp.example.com ESMTP server ready
C: EHLO jgm.example.com
S: 250-smtp.example.com
S: 250 AUTH DIGEST-MD5 EXTERNAL
C: AUTH EXTERNAL ZnJlZA==
S: 235 Authentication successful.
```

8. IANA Considerations

Registration of a SASL mechanism is done by filling in the template in [section 8.4](#) and sending it in to iana@iana.org. IANA has the right to reject obviously bogus registrations, but will perform no review of claims made in the registration form.

There is no naming convention for SASL mechanisms; any name that conforms to the syntax of a SASL mechanism name can be registered. An IETF Standards Track document may reserve a portion of the SASL mechanism namespace for its own use, amending the registration rules for that portion of the namespace.

While the registration procedures do not require it, authors of SASL mechanisms are encouraged to seek community review and comment whenever that is feasible. Authors may seek community review by posting a specification of their proposed mechanism as an internet-draft. SASL mechanisms intended for widespread use should be standardized through the normal IETF process, when appropriate.

8.1. Comments on SASL mechanism registrations

Comments on registered SASL mechanisms should first be sent to the "owner" of the mechanism. Submitters of comments may, after a reasonable attempt to contact the owner, request IANA to attach their comment to the SASL mechanism registration itself. If IANA approves of this the comment will be made accessible in conjunction with the SASL mechanism registration itself.

8.2. Location of registered SASL mechanism list

SASL mechanism registrations are available at the URL "http://www.iana.org/assignments/sasl-mechanisms". The SASL mechanism description and other supporting material may also be published as an Informational RFC by sending it to "rfc-editor@rfc-editor.org" (please follow the instructions to RFC authors [[RFC-INSTRUCTIONS](#)]).

8.3. Change control

Once a SASL mechanism registration has been published by IANA, the author may request a change to its definition. The change request follows the same procedure as the registration request.

The owner of a SASL mechanism may pass responsibility for the SASL mechanism to another person or agency by informing IANA; this can be done without discussion or review.

The IESG may reassign responsibility for a SASL mechanism. The most common case of this will be to enable changes to be made to mechanisms where the author of the registration has died, moved out of contact or is otherwise unable to make changes that are important to the community.

SASL mechanism registrations may not be deleted; mechanisms which are no longer believed appropriate for use can be declared OBSOLETE by a

change to their "intended use" field; such SASL mechanisms will be clearly marked in the lists published by IANA.

The IESG is considered to be the owner of all SASL mechanisms which are on the IETF standards track.

8.4. Registration template

To: iana@isi.edu

Subject: Registration of SASL mechanism X

SASL mechanism name:

Security considerations:

Published specification (optional, recommended):

Person & email address to contact for further information:

Intended usage:

(One of COMMON, LIMITED USE or OBSOLETE)

Owner/Change controller:

(Any other information that the author deems interesting may be added below this line.)

8.5. The EXTERNAL mechanism registration

It is requested that the SASL Mechanism registry [[IANA-SASL](#)] entry for the EXTERNAL mechanism be updated to reflect that this document now provides its technical specification.

To: iana@iana.org

Subject: Updated Registration of SASL mechanism EXTERNAL

SASL mechanism name: EXTERNAL

Security considerations: See RFC XXXX, [section 10](#).

Published specification (optional, recommended): RFC XXXX

Person & email address to contact for further information:

Alexey Melnikov <mel@isode.com>

Intended usage: COMMON

Owner/Change controller: IESG <iesg@ietf.org>

Note: Updates existing entry for EXTERNAL

9. References

9.1. Normative References

[ABNF] Crocker, Overell, "Augmented BNF for Syntax Specifications: ABNF", [RFC 2234](#), November 1997

[CHARSET-POLICY] Alvestrand, "IETF Policy on Character Sets and Languages", [RFC 2277](#), January 1998

[GSSAPI] Linn, "Generic Security Service Application Program Interface, Version 2, Update 1", [RFC 2743](#), January 2000

[ISO-10646] "Universal Multiple-Octet Coded Character Set (UCS) - Architecture and Basic Multilingual Plane", ISO/IEC 10646-1 : 1993.

[KEYWORDS] Bradner, "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), March 1997

[Stringprep] P. Hoffman, M. Blanchet, "Preparation of Internationalized Strings ("stringprep")", [RFC 3454](#), December 2002.

[SASLPrep] Zeilenga, K., "SASLprep: Stringprep profile for user names and passwords", Work in progress, [draft-ietf-sasl-saslprep-XX.txt](#).

[UTF-8] Yergeau, "UTF-8, a transformation format of ISO 10646", work in progress ([draft-yergeau-rfc2279bis-XX](#)) that replaces [RFC 2279](#), January 1998

9.2. Informative References

<<Update the reference below>> [SASL-GSSAPI] Myers, "SASL GSSAPI mechanisms", work in progress, [draft-ietf-cat-sasl-gssapi-XX.txt](#), September 2000

[SASL-DIGEST] Leach, P., Newman, C., Melnikov, A., "Using Digest Authentication as a SASL Mechanism", work in progress, [draft-ietf-sasl-rfc2831bis-XX.txt](#), replaces [RFC 2831](#)

[SASL-OTP] Newman, "The One-Time-Password SASL Mechanism", [RFC 2444](#), October 1998

[SMTP-AUTH] Myers, "SMTP Service Extension for Authentication", [RFC 2554](#), March 1999

[RFC-INSTRUCTIONS] Postel, Reynolds, "Instructions to RFC Authors", [RFC 2223](#), October 1997

[IANA-SASL] IANA, "SIMPLE AUTHENTICATION AND SECURITY LAYER (SASL) MECHANISMS", <http://www.iana.org/assignments/sasl-mechanisms>.

10. Security considerations

Security issues are discussed throughout this memo.

The mechanisms that support integrity protection are designed such that the negotiation of the security layer and authorization identity is integrity protected. When the client selects a security layer with at least integrity protection, this protects against an active attacker hijacking the connection and modifying the authentication exchange to negotiate a plaintext connection.

When a server or client supports multiple authentication mechanisms, each of which has a different security strength, it is possible for an active attacker to cause a party to use the least secure mechanism supported. To protect against this sort of attack, a client or server which supports mechanisms of different strengths should have a configurable minimum strength that it will use. It is not sufficient for this minimum strength check to only be on the server, since an active attacker can change which mechanisms the client sees as being supported, causing the client to send authentication credentials for its weakest supported mechanism.

The client's selection of a SASL mechanism is done in the clear and may be modified by an active attacker. It is important for any new SASL mechanisms to be designed such that an active attacker cannot obtain an authentication with weaker security properties by modifying the SASL mechanism name and/or the challenges and responses.

Any protocol interactions prior to authentication are performed in the clear and may be modified by an active attacker. In the case where a client selects integrity protection, it is important that any security-sensitive protocol negotiations be performed after authentication is complete. Protocols should be designed such that negotiations performed prior to authentication should be either ignored or revalidated once authentication is complete.

When use of a security layer is negotiated by the authentication protocol exchange, the receiver should handle gracefully any security encoded data buffer larger than the defined/negotiated maximal size. In particular, it must not blindly allocate the amount of memory specified in the buffer size field, as this might cause the "out of memory" condition. If the receiver detects a large block, it SHOULD

close the connection.

"stringprep" and Unicode security considerations apply to authentication identities, authorization identities and passwords.

The EXTERNAL mechanism provides no security protection; it is vulnerable to spoofing by either client or server, active attack, and eavesdropping. It should only be used when external security mechanisms are present and have sufficient strength.

11. Editor's Address

Alexey Melnikov
Isode

Email: mel@isode.com

12. Acknowledgments

This document is a revision of [RFC 2222](#) written by John G. Myers <jgmyers@netscape.com>. He also wrote the major part of this document.

Thank you to Magnus Nystrom for the ASCII picture used in [section 6.3](#).

Definition of realm was extracted from [RFC 2617](#) ("HTTP Authentication: Basic and Digest Access Authentication").

Contributions of many members of the SASL mailing list are gratefully acknowledged.

13. Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be

followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

[Appendix A](#). Relation of SASL to transport security

Questions have been raised about the relationship between SASL and various services (such as IPsec and TLS) which provide a secured connection.

Two of the key features of SASL are:

The separation of the authorization identity from the identity in the client's credentials. This permits agents such as proxy servers to authenticate using their own credentials, yet request the access privileges of the identity for which they are proxying.

Upon successful completion of an authentication exchange, the server knows the authorization identity the client wishes to use. This allows servers to move to a "user is authenticated" state in the protocol.

These features are extremely important to some application protocols, yet Transport Security services do not always provide them. To define SASL mechanisms based on these services would be a very messy task, as the framing of these services would be redundant with the framing of SASL and some method of providing these important SASL features would have to be devised.

Sometimes it is desired to enable within an existing connection the use of a security service which does not fit the SASL model. (TLS is an example of such a service.) This can be done by adding a command, for example "STARTTLS", to the protocol. Such a command is outside the scope of SASL, and should be different from the command which

starts a SASL authentication protocol exchange.

In certain situations, it is reasonable to use SASL underneath one of these Transport Security services. The transport service would secure the connection, either service would authenticate the client, and SASL would negotiate the authorization identity. The SASL negotiation would be what moves the protocol from "unauthenticated" to "authenticated" state. The "EXTERNAL" SASL mechanism is explicitly intended to handle the case where the transport service secures the connection and authenticates the client and SASL negotiates the authorization identity.

When using SASL underneath a sufficiently strong Transport Security service, a SASL security layer would most likely be redundant. The client and server would thus probably want to negotiate off the use of a SASL security layer.

Appendix B. IANA considerations

The IANA is directed to modify the SASL mechanisms registry as follows:

Change the "Intended usage" of the KERBEROS_V4 and SKEY mechanism registrations to OBSOLETE. Change the "Published specification" of the EXTERNAL mechanism to this document.

Appendix C. Changes since [RFC 2222](#)

The GSSAPI mechanism was removed. It is now specified in a separate document [SASL-GSSAPI].

The "KERBEROS_V4" mechanism defined in [RFC 2222](#) is obsolete and has been removed.

The "SKEY" mechanism described in [RFC 2222](#) is obsolete and has been removed. It has been replaced by the OTP mechanism [[SASL-OTP](#)].

The overview has been substantially reorganized and clarified.

Clarified the definition and semantics of the authorization identity.

Prohibited the NULL character in authorization identities.

Added a section on character string issues.

The word "must" in the first paragraph of the "Protocol profile requirements" section was changed to "MUST".

Specified that protocol profiles SHOULD provide a way for clients to discover available SASL mechanisms.

Made the requirement that protocol profiles specify the semantics of the authorization identity optional to the protocol profile.
Clarified that such a specification is a refinement of the definition in the base SASL spec.

Added a requirement discouraging protocol profiles from breaking the separation between protocol and mechanism.

Mentioned that standards track documents may carve out their own portions of the SASL mechanism namespace.

Specified that the authorization identity in the EXTERNAL mechanism is encoded in UTF-8.

Added a statement that a protocol profile SHOULD allow challenge data to be sent with a success indication.

Added a security consideration for the EXTERNAL mechanism.

Clarified sections concerning success with additional data.

Updated IANA related URLs.

Updated references and split them into Informative and Normative.

Added text to the Security Considerations section regarding handling of extremely large SASL blocks.

Replaced UTF-8 ABNF with the reference to the UTF-8 document.

Added text about SASLPrep for authentication identities and passwords.

Added paragraph about verifying authorization identities.

This document requires to drop a security layer on reauthentication when no security layer is negotiated. This differs from [RFC 2222](#), which required to keep the last security layer in this case.

Added a protocol profile requirement to specify interaction between SASL and TLS security layers.

Status of this Memo	i
1. Abstract	2
2. Organization of this document	2
2.1. How to read this document	2
2.2. Conventions used in this document	2
3. Overview	2
4. Authentication mechanisms	3
4.1. Authentication protocol exchange	4
4.2. Authorization identities and proxy authentication	4
4.3. Security layers	5
4.4. Character string issues	6
5. Protocol profile requirements	6
6. Specific issues	8
6.1. Client sends data first	8
6.2. Server returns success with additional data	8
6.3. Multiple authentications	9
7. The EXTERNAL mechanism	10
7.1. Formal syntax	11
7.2. Example	11
8. IANA Considerations	11
8.1. Comments on SASL mechanism registrations	12
8.2. Location of registered SASL mechanism list	12
8.3. Change control	12
8.4. Registration template	13
8.5. The EXTERNAL mechanism registration	13
9. References	14
9.1. Normative References	14
9.2. Informative References	14
10. Security considerations	15
11. Editor's Address	16
12. Acknowledgments	16
13. Full Copyright Statement	16
Appendix A. Relation of SASL to transport security	17
Appendix B. IANA considerations	18
Appendix C. Changes since RFC 2222	18

