Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 5 November 2026

R. Robert
Phoenix R&D
C. A. Wood
Cloudflare
T. Meunier
Cloudflare Inc.

4 May 2026

Batched Token Issuance Protocol
draft-ietf-privacypass-batched-tokens-08

Abstract

This document specifies two variants of the Privacy Pass issuance protocol that allow for batched issuance of tokens. These allow clients to request more than one token at a time and for issuers to issue more than one token at a time.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 5 November 2026.

Table of Contents

1. Change Log:

RFC EDITOR PLEASE DELETE THIS SECTION.

draft-07

* Add some precision on linear cost of amortized batched tokens

draft-06

* Address various review comments

draft-05

* Address various review comments

draft-04

* Rename the issuance variants

* Clarify media types

* Make generic issuance more generic byt prefixing requests & responses with token type

draft-03

* Arbitrary token types

* Error code 400 aligned with RFC9578 and replaced by error code 422

draft-02

* Renaming TokenRequest to BatchTokenRequest and TokenResponse to BatchTokenResponse

* IANA: Media types for BatchTokenRequest and BatchTokenResponse

* IANA: Expand Token Type registry entry

* Various editorial fixes

draft-01

* Initial WG document version

2. Introduction

This document specifies two variants of Privacy Pass issuance protocols (as defined in [RFC9576]) that allow for batched issuance of tokens. This allows clients to request more than one token at a time and for issuers to issue more than one token at a time.

The base Privacy Pass issuance protocol [RFC9578] defines stateless anonymous tokens, which can either be publicly verifiable or not. While it is possible to run multiple instances of the issuance protocol in parallel, e.g., over a multiplexed transport such as HTTP/3 [HTTP3] or by orchestrating multiple HTTP requests, these ad-hoc solutions vary based on transport protocol support. In addition, in some cases, they cannot take advantage of cryptographic optimizations.

The first variant (Section 5) of the issuance protocol builds upon the privately verifiable issuance protocol in [RFC9578] that uses VOPRF [OPRF], and allows for batched issuance of tokens and amortizes the cost of zero knowledge proofs. This allows clients to request more than one token at a time and for issuers to issue more than one token at a time. In effect, amortizing private batched issuance reduces the per-token cost, approaching a factor of 2 for large batches.

The second variant (Section 6) of the issuance protocol introduces a new Client-Issuer communication method, which allows for batched issuance of generic token types. This allows clients to request more than one token at a time and for issuers to issue more than one token at a time. This variant has no other effect than batching requests and responses and the issuance performance remains linear.

This document registers a new token type (Section 8.1) that can either be used with the Privately Verifiable Issuance Protocol as defined in [RFC9578], or with the Amortized Privately Verifiable Batch Issuance Protocol defined below.

2.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Motivation

Privacy Pass tokens (as defined in [RFC9576] and [RFC9578]) are unlinkable during issuance and redemption. The basic issuance protocols defined in [RFC9578], however, only allow for a single token to be issued at a time for every challenge. In some cases, especially where a large number of clients need to fetch a large number of tokens, this may introduce performance bottlenecks.

Amortized Privately Verifiable Token Issuance Section 5 improves upon the basic Privately Verifiable Token issuance protocol in the following key ways:

1. Issuing multiple tokens at once in response to a single TokenChallenge, thereby reducing the size of the proofs required for multiple tokens.

2. Improving server and client issuance efficiency by amortizing the cost of the VOPRF proof generation and verification, respectively.

Generic Token Batch Issuance Section 6 allows for a single GenericBatchTokenRequest to be sent that encompasses multiple token requests. This improves upon the basic issuance protocols defined in [RFC9578] in the following key ways:

1. Issuing multiple tokens at once of the same type with different keys.

2. Issuing multiple tokens at once of different types.

4. Presentation Language

This document uses the TLS presentation language [RFC8446] to describe the structure of protocol messages. In addition to the base syntax, it uses two additional features: the ability for fields to be optional and the ability for vectors to have variable-size length headers.

4.1. Optional Value

An optional value is encoded with a presence-signaling octet, followed by the value itself if present. When decoding, a presence octet with a value other than 0 or 1 MUST be rejected as malformed.

```
struct {
    uint8 present;
    select (present) {
        case 0: struct{};
        case 1: T value;
    };
} optional<T>;
```

4.2. Variable-Size Vector Length Headers

In the TLS presentation language, vectors are encoded as a sequence of encoded elements prefixed with a length. The length field has a fixed size set by specifying the minimum and maximum lengths of the encoded sequence of elements.

In this document, there are several vectors whose sizes vary over significant ranges. So instead of using a fixed-size length field, it uses a variable-size length using a variable-length integer encoding based on the one described in Section 16 of [RFC9000]. They differ only in that the one here requires a minimum-size encoding. Instead of presenting min and max values, the vector description simply includes a V. For example:

```
struct {
    uint32 fixed<0..255>;
    opaque variable<V>;
} StructWithVectors;
```

5. Amortized Privately Verifiable Token Batch Issuance

This section describes a batched issuance protocol for select token types, including 0x0001 (defined in [RFC9578]) and 0x0005 (defined in this document). This variant is more efficient than Generic Token Batch Issuance defined below. It does so by requiring the same key to be used by all token requests.

5.1. Client-to-Issuer Request

Except where specified otherwise, the client follows the same protocol as described in [RFC9578], Section 5.1.

The Client first creates a context as follows:

```
client_context = SetupVOPRFClient(ciphersuiteID, pkI)
```

ciphersuiteID is the ciphersuite identifier from [OPRF] corresponding to the ciphersuite being used for this token version. SetupVOPRFClient is defined in [OPRF], Section 3.2.

Nr denotes the number of tokens the clients wants to request. For every token, the Client then creates an issuance request message for a random value nonce with the input challenge and Issuer key identifier as described below:

```
nonce_i = random(32)
challenge_digest = SHA256(challenge)
token_input = concat(token_type, nonce_i, challenge_digest,
                token_key_id)
blind_i, blinded_element_i = client_context.Blind(token_input)
```

token_type corresponds to the 2-octet integer in the challenge.

The above is repeated for each token to be requested. Importantly, a fresh nonce MUST be sampled each time.

The Client then creates a BatchTokenRequest structured as follows:

```
struct {
    uint8_t blinded_msg[Ne];
} BlindedMessage;

struct {
    uint16_t token_type;
    uint8_t truncated_token_key_id;
    BlindedMessage blinded_msgs<V>;
} AmortizedBatchTokenRequest;
```

The structure fields are defined as follows:

* "token_type" is a 2-octet integer, which matches the type in the challenge.

* "truncated_token_key_id" is the least significant byte of the token_key_id in network byte order (in other words, the last 8 bits of token_key_id).

* "blinded_msgs" is a list of Nr serialized elements, each of length Ne bytes and computed as SerializeElement(blinded_element_i), where blinded_element_i is the i-th output sequence of Blind invocations above. Ne is as defined in [OPRF], Section 4.

The Client then generates an HTTP POST request to send to the Issuer Request URL, with the AmortizedBatchTokenRequest as the content. The media type for this request MUST be "application/private-token-amortized-batch-request". If not, the Issuer responds with status code 415. An example request for the Issuer Request URL "https://issuer.example.net/request" is shown below.

```
POST /request HTTP/1.1
Host: issuer.example.net
Accept: application/private-token-amortized-batch-response
Content-Type: application/private-token-amortized-batch-request
Content-Length: <Length of AmortizedBatchTokenRequest>

<Bytes containing the AmortizedBatchTokenRequest>
```

5.2. Issuer-to-Client Response

Except where specified otherwise, the client follows the same protocol as described in [RFC9578], Section 5.2.

Upon receipt of the request, the Issuer validates the following conditions:

* The AmortizedBatchTokenRequest contains a supported token_type of the privately verifiable token kind.

* The AmortizedBatchTokenRequest.truncated_token_key_id corresponds to a key ID of a Public Key owned by the issuer.

* Nr, as determined based on the size of AmortizedBatchTokenRequest.blinded_msgs, is less than or equal to the number of tokens that the issuer can issue in a single batch.

If any of these conditions is not met, the Issuer MUST return an HTTP 422 (Unprocessable Content) error to the client.

The Issuer then tries to deseralize the i-th element of AmortizedBatchTokenRequest.blinded_msgs using DeserializeElement from Section 2.1 of [OPRF], yielding blinded_element_i of type Element. If this fails for any of the AmortizedBatchTokenRequest.blinded_msgs values, the Issuer MUST return an HTTP 422 (Unprocessable Content) error to the client. Otherwise, if the Issuer is willing to produce a token to the Client, the issuer forms a list of Element values, denoted blinded_elements, and computes a blinded response as follows:

```
server_context = SetupVOPRFServer(ciphersuiteID, skI, pkI)

evaluated_elements, proof =
  BlindEvaluateBatch(skI, pkI, blinded_elements)
```

ciphersuiteID is the ciphersuite identifier from [OPRF] corresponding to the ciphersuite being used for this token version. SetupVOPRFServer is defined in [OPRF], Section 3.2. The issuer uses a list of blinded elements to compute in the proof generation step. The BlindEvaluateBatch function is a batch-oriented version of the BlindEvaluate function described in [OPRF], Section 3.3.2. The description of BlindEvaluateBatch is below.

Input:

```
Scalar skS
Element pkS
Element blindedElements[Nr]
```

Output:

```
Element evaluatedElements[Nr]
Proof proof
```

Parameters:

```
Group G
```

```
def BlindEvaluateBatch(skS, pkS, blindedElements):
  evaluatedElements = []
  for blindedElement in blindedElements:
    evaluatedElements.append(skS * blindedElement)

  proof = GenerateProof(skS, G.Generator(), pkS,
                        blindedElements, evaluatedElements)
  return evaluatedElements, proof
```

The computational complexity of BlindEvaluateBatch is linear in the number of evaluations Nr. However the amortization of proof generation across all Nr evaluations reduces the practical cost by approximately half that of Nr individual token issuance operations as Nr increases.

The Issuer then creates a AmortizedBatchTokenResponse structured as follows:

```
struct {
    uint8_t evaluated_msg[Ne];
} EvaluatedMessage;

struct {
    EvaluatedMessage evaluated_msgs<V>;
    uint8_t evaluated_proof[Ns + Ns];
} AmortizedBatchTokenResponse;
```

The structure fields are defined as follows:

* "evaluated_msgs" is a list of Nr serialized elements, each of length Ne bytes and computed as SerializeElement(evaluated_element_i), where evaluated_element_i is the i-th output of BlindEvaluate.

* "evaluated_proof" is the (Ns+Ns)-octet serialized proof, which is a pair of Scalar values, computed as concat(SerializeScalar(proof[0]), SerializeScalar(proof[1])), where Ns is as defined in [OPRF], Section 4.

The Issuer MUST generate an HTTP response with status code 200 whose content consists of AmortizedBatchTokenResponse, with the content type set as "application/private-token-amortized-batch-response". Clients MUST ignore the response if the status code is not 200 or if the content type is not "application/private-token-amortized-batch-response".

```
HTTP/1.1 200 OK
Content-Type: application/private-token-amortized-batch-response
Content-Length: <Length of AmortizedBatchTokenResponse>

<Bytes containing the AmortizedBatchTokenResponse>
```

5.3. Finalization

Upon receipt, the Client handles the response and, if successful, deserializes the body values AmortizedBatchTokenResponse.evaluated_msgs and AmortizedBatchTokenResponse.evaluated_proof, yielding evaluated_elements and proof. If deserialization of either value fails, the Client aborts the protocol. Otherwise, the Client processes the response as follows:

```
authenticator_values = client_context.FinalizeBatch(token_input, blind,
                         evaluated_elements, blinded_elements, proof)
```

The FinalizeBatch function is a batched variant of the Finalize function as defined in [OPRF], Section 3.3.2. FinalizeBatch accepts lists of evaluated elements and blinded elements as input parameters, and is implemented as described below:

```
Input:

  PrivateInput input
  Scalar blind
  Element evaluatedElements[Nr]
  Element blindedElements[Nr]
  Element pkS
  Proof proof

Output:

  opaque output[Nh * Nr]

Parameters:

  Group G

Errors: VerifyError

def FinalizeBatch(input, blind,
  evaluatedElements, blindedElements, pks, proof):
  if VerifyProof(G.Generator(), pkS, blindedElements,
                 evaluatedElements, proof) == false:
    raise VerifyError

  output = nil
  for evaluatedElement in evaluatedElements:
    N = G.ScalarInverse(blind) * evaluatedElement
    unblindedElement = G.SerializeElement(N)
    hashInput = I2OSP(len(input), 2) || input ||
                I2OSP(len(unblindedElement), 2) || unblindedElement ||
                "Finalize"
    output = concat(output, Hash(hashInput))

  return output
```

If this succeeds, the Client then constructs Nr Token values, where authenticator is the i-th Nh-byte length slice of authenticator_values that corresponds to nonce, the i-th nonce that was sampled in Section 5.1:

```
struct {
    uint16_t token_type; /* 0x0001 or 0x0005 */
    uint8_t nonce[32];
    uint8_t challenge_digest[32];
    uint8_t token_key_id[32];
    uint8_t authenticator[Nh];
} Token;
```

The constant Nh is as defined in [OPRF], Section 4 and denotes the output length of the hash function in bytes used by the token type.

If the FinalizeBatch function fails, the Client aborts the protocol. Token verification works exactly as specified in [RFC9578].

6. Generic Token Batch Issuance

This section describes an issuance protocol mechanism for issuing multiple tokens in one round trip between Client and Issuer. A generic batch token request can contain token requests for any token type.

6.1. Client-to-Issuer Request

The Client first generates all of the individual TokenRequest structures that are intended to be batched together. This request creation follows the protocol describing issuance, such as [RFC9578], Section 5.1 or [RFC9578], Section 6.1.

The Client then creates a GenericBatchedTokenRequest structure as follows:

```
struct {
    uint16_t token_type;
    select (token_type) {
        case (0x0001): /* Type VOPRF(P-384, SHA-384), RFC 9578 */
            TokenRequest token_request;
        case (0x0002): /* Type Blind RSA (2048-bit), RFC 9578 */
            TokenRequest token_request;
        case (0x0005): /* Type VOPRF(ristretto255, SHA-512), this document */
            TokenRequest token_request;
        case (other): /* Other token types from the IANA Privacy Pass Token Types Regi
stry */
            TokenRequest token_request;
    }
} GenericTokenRequest;

struct {
    GenericTokenRequest generic_token_requests<V>;
} GenericBatchTokenRequest
```

The structure fields are defined as follows:

* GenericTokenRequest's "token_type" is a 2-octet integer. The value represents the token type from the IANA Privacy Pass Token Types Registry ([IANA_PRIVACYPASS_TOKEN_TYPES]). The rest of the structure follows with the TokenRequest based on that type.

* "token_requests" is an array of GenericTokenRequest satisfying the above constraint.

The Client then generates an HTTP POST request to send to the Issuer Request URL, with the GenericBatchTokenRequest as the content. The media type for this request MUST be "application/private-token-generic-batch-request". If not, the Issuer responds with status code 415. An example request for the Issuer Request URL "https://issuer.example.net/request" is shown below.

```
POST /request HTTP/1.1
Host: issuer.example.net
Accept: application/private-token-generic-batch-response
Content-Type: application/private-token-generic-batch-request
Content-Length: <Length of GenericBatchTokenRequest>

<Bytes containing the GenericBatchTokenRequest>
```

6.2. Issuer-to-Client Response

Upon receipt of the request, the Issuer validates the following conditions:

* The Content-Type is application/private-token-generic-batch-request as registered with IANA.

If this condition is not met, the Issuer MUST return an HTTP 422 (Unprocessable Content) error to the client.

The Issuer then tries to deserialize the first 2 bytes of the i-th element of GenericBatchTokenRequest.token_requests. If this is not a token type registered with IANA, the Issuer MUST return an HTTP 422 (Unprocessable Content) error to the client. The issuer creates a GenericBatchTokenResponse structured as follows:

```
struct {
    uint16_t token_type;
    select (token_type) {
        case (0x0001): /* Type VOPRF(P-384, SHA-384), RFC 9578 */
            TokenResponse token_response;
        case (0x0002): /* Type Blind RSA (2048-bit), RFC 9578 */
            TokenResponse token_response;
        case (0x0005): /* Type VOPRF(ristretto255, SHA-512), this document */
            TokenResponse token_response;
        case (other): /* Other token types */
            TokenResponse token_response;
    }
} GenericTokenResponse;

struct {
    optional<GenericTokenResponse> generic_token_response; /* Defined by token_type */
} OptionalTokenResponse;

struct {
    OptionalTokenResponse optional_token_responses<V>;
} GenericBatchTokenResponse
```

For each request in GenericBatchTokenRequest.token_requests, the issuer generates a TokenResponse according to the token type. GenericBatchTokenResponse.optional_token_responses is a variable-size vector of OptionalTokenResponses. OptionalTokenResponse.token_response is an optional TokenResponse (as specified in Section 4.1), where an absence of TokenResponse indicates that the Issuer failed or refused to issue the associated TokenRequest.

The Issuer MUST generate an HTTP response with status code 200 whose content consists of TokenResponse, with the content type set as "application/private-token-generic-batch-response". Clients MUST ignore the response if the status code is not 200, 206 or if the content type is not "application/private-token-generic-batch-response".

```
HTTP/1.1 200 OK
Content-Type: application/private-token-generic-batch-response
Content-Length: <Length of GenericBatchTokenResponse>

<Bytes containing the GenericBatchTokenResponse>
```

If the Issuer issues some but not all tokens, it MUST return an HTTP 206 Partial Content response defined in Section 15.3.7 of [RFC9110] to the client and continue processing subsequent requests. For instance, an Issuer MAY return an HTTP 206 error if requests for tokens of the same token type refer to more than one truncated_token_key_id.

If the Issuer decides not to issue any tokens, it MUST return an HTTP 400 Bad Request as defined in Section 15.5.1 of [RFC9110] to the client.

6.3. Finalization

The Client tries to deserialize the i-th element of GenericBatchTokenResponse.token_responses using the protocol associated to GenericBatchTokenRequest.token_type. If the element has a size of 0, the Client MUST ignore this token, and continue processing the next token. The Client finalizes each deserialized TokenResponse using the matching TokenRequest according to the corresponding finalization procedure defined by the token type.

7. Security considerations

7.1. Amortized Privately Verifiable Token Batch Issuance

Implementors SHOULD be aware of the security considerations described in [OPRF], Section 6.2.3 and implement mitigation mechanisms. Application can mitigate this issue by limiting the number of clients and limiting the number of token requests per client per key.

7.2. Generic Token Batch Issuance

Implementors SHOULD be aware of the inherent linear cost of this token type. An Issuer MAY ignore GenericTokenRequest if the number of tokens per request is past a limit.

8. IANA considerations

This section contains IANA codepoint allocation requests.

8.1. Token Type

This document updates the "Token Type" Registry (Section 6.2 of [AUTHSCHEME]) with the following entry:

* Value: 0x0005 (suggested)

* Name: VOPRF (ristretto255, SHA-512)

* Token Structure: As defined in Section 2.2 of [AUTHSCHEME]

* Token Key Encoding: Serialized using SerializeElement from Section 2.1 of [OPRF]

* TokenChallenge Structure: As defined in Section 2.1 of [AUTHSCHEME]

* Publicly Verifiable: N

* Public Metadata: N

* Private Metadata: N

* Nk: 64

* Nid: 32

* Change controller: IETF

* Reference: [RFC9578], Section 5

* Notes: None

8.2. Media Types

The following entries should be added to the IANA "media types" registry:

* "application/private-token-amortized-batch-request"

* "application/private-token-amortized-batch-response"

* "application/private-token-generic-batch-request"

* "application/private-token-generic-batch-response"

The templates for these entries are listed below and the reference should be this RFC.

8.2.1. "application/private-token-amortized-batch-request" media type

Type name: application
Subtype name: private-token-amortized-batch-request
Required parameters: N/A
Optional parameters: N/A
Encoding considerations: "binary"
Security considerations: see Section 7

Interoperability considerations: N/A
Published specification: this specification
Applications that use this media type: Applications that want to issue or facilitate issuance of Privacy Pass Amortized Privately Verifiable tokens as defined in Section 5, including Privacy Pass issuer applications themselves.
Fragment identifier considerations: N/A
Additional information: Magic number(s): N/A
Deprecated alias names for this type: N/A
File extension(s): N/A
Macintosh file type code(s): N/A
Person and email address to contact for further information: see Authors' Addresses section
Intended usage: COMMON
Restrictions on usage: N/A
Author: see Authors' Addresses section
Change controller: IETF

8.2.2. "application/private-token-amortized-batch-response" media type

Type name: application
Subtype name: private-token-amortized-batch-response
Required parameters: N/A
Optional parameters: N/A
Encoding considerations: "binary"
Security considerations: see Section 7
Interoperability considerations: N/A
Published specification: this specification
Applications that use this media type: Applications that want to issue or facilitate issuance of Privacy Pass Amortized Privately Verifiable tokens as defined in Section 5, including Privacy Pass issuer applications themselves.
Fragment identifier considerations: N/A
Additional information: Magic number(s): N/A
Deprecated alias names for this type: N/A
File extension(s): N/A
Macintosh file type code(s): N/A
Person and email address to contact for further information: see Authors' Addresses section
Intended usage: COMMON
Restrictions on usage: N/A
Author: see Authors' Addresses section
Change controller: IETF

8.2.3. "application/private-token-generic-batch-request" media type

Type name: application
Subtype name: private-token-generic-batch-request

Required parameters: N/A
Optional parameters: N/A
Encoding considerations: "binary"
Security considerations: see Section 7
Interoperability considerations: N/A
Published specification: this specification
Applications that use this media type: Applications that want to issue or facilitate issuance of Privacy Pass Generic tokens as defined in Section 6, including Privacy Pass issuer applications themselves.
Fragment identifier considerations: N/A
Additional information: Magic number(s): N/A
Deprecated alias names for this type: N/A
File extension(s): N/A
Macintosh file type code(s): N/A
Person and email address to contact for further information: see Authors' Addresses section
Intended usage: COMMON
Restrictions on usage: N/A
Author: see Authors' Addresses section
Change controller: IETF

8.2.4. "application/private-token-generic-batch-response" media type

Type name: application
Subtype name: private-token-generic-batch-response
Required parameters: N/A
Optional parameters: N/A
Encoding considerations: "binary"
Security considerations: see Section 7
Interoperability considerations: N/A
Published specification: this specification
Applications that use this media type: Applications that want to issue or facilitate issuance of Privacy Pass Generic tokens as defined in Section 6, including Privacy Pass issuer applications themselves.
Fragment identifier considerations: N/A
Additional information: Magic number(s): N/A
Deprecated alias names for this type: N/A
File extension(s): N/A
Macintosh file type code(s): N/A
Person and email address to contact for further information: see Authors' Addresses section
Intended usage: COMMON
Restrictions on usage: N/A
Author: see Authors' Addresses section
Change controller: IETF

9. References

9.1. Normative References

[AUTHSCHEME] Pauly, T., Valdez, S., and C. A. Wood, "The Privacy Pass HTTP Authentication Scheme", RFC 9577, DOI 10.17487/RFC9577, June 2024, <https://www.rfc-editor.org/rfc/rfc9577>.

[OPRF] Davidson, A., Faz-Hernandez, A., Sullivan, N., and C. A. Wood, "Oblivious Pseudorandom Functions (OPRFs) Using Prime-Order Groups", RFC 9497, DOI 10.17487/RFC9497, December 2023, <https://www.rfc-editor.org/rfc/rfc9497>.

[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/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

[RFC9110] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "HTTP Semantics", STD 97, RFC 9110, DOI 10.17487/RFC9110, June 2022, <https://www.rfc-editor.org/rfc/rfc9110>.

[RFC9576] Davidson, A., Iyengar, J., and C. A. Wood, "The Privacy Pass Architecture", RFC 9576, DOI 10.17487/RFC9576, June 2024, <https://www.rfc-editor.org/rfc/rfc9576>.

[RFC9578] Celi, S., Davidson, A., Valdez, S., and C. A. Wood, "Privacy Pass Issuance Protocols", RFC 9578, DOI 10.17487/RFC9578, June 2024, <https://www.rfc-editor.org/rfc/rfc9578>.

9.2. Informative References

[HTTP3] Bishop, M., Ed., "HTTP/3", RFC 9114, DOI 10.17487/RFC9114, June 2022, <https://www.rfc-editor.org/rfc/rfc9114>.

[IANA_PRIVACYPASS_TOKEN_TYPES]
"IANA Privacy Pass Token Types Registry", n.d., <https://www.iana.org/assignments/privacy-pass/privacy-pass.xhtml#token-type>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/rfc/rfc9000>.

Appendix A. Test Vectors

This section includes test vectors for the two issuance protocols specified in this document. Appendix A.3 contains test vectors for Amortized Privately Verifiable Token Batch Issuance (0x0005), and Appendix A.4 contains test vectors for Generic Token Batch Issuance.

A.1. Privately Verifiable Token Issuance - VOPRF (ristretto255, SHA-512)

The test vectors below list the following values:

* skS: The Issuer Private Key, serialized using SerializeScalar (Section 2.1 of [OPRF]) and represented as a hexadecimal string.

* pkS: The Issuer Public Key, serialized according to the encoding in Section 8.1.

* token_challenge: A randomly generated TokenChallenge structure, represented as a hexadecimal string. nonce: The 32-byte Client nonce generated according to Section 5.1, represented as a hexadecimal string. blind: The blind used when computing the OPRF blinded message, serialized using SerializeScalar (Section 2.1 of [OPRF]) and represented as a hexadecimal string. token_request: The TokenRequest message constructed according to Section 5.1, represented as a hexadecimal string. token_response: The TokenResponse message constructed according to Section 5.2, represented as a hexadecimal string. token: The output token from the protocol, represented as a hexadecimal string.

```
// Test vector 1:
skS:
065cca6457eac53b38c4f174ea1498fee99bb0c724035e1ed0baace5c3223201
pkS:
28c68b4c454bb67e0138e2ca3ce77a4a92bb570de7023a1d0fc885f9b6fa7d44
token_challenge: 0005000e6973737565722e6578616d706c65208278149d30
94c9138347d7a2bcbf1188a262a10b1a5696c41549eabed84c129d000e6f72696
7696e2e6578616d706c65
```

```
   nonce:
   678dd032dc3dd290a524c9525b59e9fa2a1426f2ebe07d71be44e410235c5bc9
   blind:
   f16cd9d7b9618a5a434439f6edd5e5d053f2781f90169eb4057ef94b65a9f900
   token_request: 0005a3987bcba79eb7bb4afbdd3acd2500417f68eb109b420f
   871ae0964481d1cfc64c
   token_response: a85598dd8eeb0e4e8ad61672a1b60cb879dcb6e2bb577f53a
   6c5799605adad73fc085894a651a29be45d10431eb3a60948f594eb1a0b82fdb2
   1fa1bcba1bd20e7e16d160b6ae31c1e3b612145b406920f9d206a2213b8b13bee
   a076c2ed4dd05
   token: 0005678dd032dc3dd290a524c9525b59e9fa2a1426f2ebe07d71be44e4
   10235c5bc9ead0d1e696ccbef94da0dd33e0e265d97a8015532f429d968fa41fb
   0af0cb38547fe05e1fd8dac4eb493924ea617a4d5b950e2d6deec99806bce0589
   29d0d3a386b38c783958b8f975795b2e3544cb58ea24eadb236c970641bb27509
   5aedfa5da76bb808f55ba51aa407be433d5598fe708cfc3d2a1f6c9b40fa9d9a7
   fa65c5

   // Test vector 2:
   skS:
   9f24660c54374169e9605c7c5431ff93547ec2a5de0a6a5f4178720be1c6a00f
   pkS:
   fa1a06593483ef048e77d54214697dc5734672bb927db0b3c7e08b6db8adce4b
   token_challenge: 0005000e6973737565722e6578616d706c6500000e6f7269
   67696e2e6578616d706c65
   nonce:
   1543cf07d8f64f9163b2487376e3e23aa36224b64b56d982838ef6a2f5a0c32a
   blind:
   e3632369f86f13da22089761dae12c829fcc7d9c7f41ca8b072a2765104a7e05
   token_request: 00051e4a0ef58c0f18db88f5fa97324cce8e8c642d92bfc452
   5a58bb857a51c4b9645a
   token_response: 30e4110f871a6b8ef610153df24a0ce3d025979462e379c10
   3908fa5fe95c8295cc5f771b69422fe711e436a791d10fbfb86dd18300c25fcd7
   7ee0a6c72bdc022421875e5bfd78055fb79d8e6fc4c475899578127e595981030
   8738d58f7ed0b
   token: 00051543cf07d8f64f9163b2487376e3e23aa36224b64b56d982838ef6
   a2f5a0c32a69b53830c9e88ce2285efc18a8bdc36d2225a41c4afdd0ce1337411
   f9e7ec0ae50d42f2b86fe4657a5f2363d89c542d11a7e290d2c48ccf06c941dcd
   301e181eb52beac7a9bcb001e25ea61095ac7249c5923e8aedd542a608362d65d
   59c3bcd3a53c0f1910be2de4c746f2846f722d07dd239b0d193c670bb4eea1b01
   d4a978

   // Test vector 3:
   skS:
   57a14d07df82a820c9c9d01386ef80850ef61690cea21432bec1366d6d997200
   pkS:
   184f826f89d9349e78d71715f1e3e91e51ecaa4a307def65905ce3ac76c8427c
   token_challenge: 0005000e6973737565722e6578616d706c65000017666f6f
   2e6578616d706c652c6261722e6578616d706c65
```

```
   nonce:
   ff94318c0a49c08b421888076a8bf8b8223bb25685ffacd1e8001ddb71ce874e
   blind:
   8f23a75ac79fd6361654a9d5bdb06063366c0f918c0dfeb18b2aaa4046a8300f
   token_request: 0005d90c8f332d31ac1fafc4d4efbb10d83a56e0c4db0bd3da
   a729e7123522bfa76c4e
   token_response: 30fc1468e7e0fc9ed1d58df1b781c4a12a65b0ffb05ecaf6e
   642e678259cf944c1201fffd9382d149def2b36a24ad5eab8daf39878ce24b3a3
   b33d0a9088f5000a25afc2c442a5caef39d55d862b267f59d575ac2e190990cec
   c9111414d2203
   token: 0005ff94318c0a49c08b421888076a8bf8b8223bb25685ffacd1e8001d
   db71ce874e8a73b15843d93251b73e17d484d3e5467e6db28a74a042d83a31100
   5dfdb9c61d38db1eae5d88760e75355ff0060861137b5e5a45bd6e64e8d3da4f5
   e38155d98c06ff991b907b45d512d5f4cb39aeef67c0d6e738792e1457e29c140
   2bf5feb4c55f0337aa7f73dc366fcdf8d2c9b823bb99ba2efe39ab31fa4d561e8
   dbb408

   // Test vector 4:
   skS:
   14b3821a3b383d384141a8135191944d74b07371fb78a465521f0867b7628006
   pkS:
   4429d3c5dbc68f9280dfde3ceeb4bcc0da37c681b83065a7319e16c886d4c856
   token_challenge: 0005000e6973737565722e6578616d706c65000000
   nonce:
   a53148ef0e37785a51950efc46ee1c959a9f2511f8d5570dfcd609d3001a1dbd
   blind:
   d85f5a0096304a954d4d7feba0faaa3011a004337d70197b3b607547ed2e6508
   token_request: 0005f656c94386183dee559fee3953b04fb9b97dcad9b5bc1e
   1ec8d2513804e8f71b03
   token_response: 6c2c459fe0975d59d4f38dcf26f81dfc28a83d45840897da0
   3d729e805867843aae4c66edae05f2fce4b755d41c245e0841aff2a61e1525156
   55b03eee2cab00660a5c9d4263f83e6e4cd9c7ce7ec7c0b4dd45b6fa8ae9b2d1c
   ff124273e6d00
   token: 0005a53148ef0e37785a51950efc46ee1c959a9f2511f8d5570dfcd609
   d3001a1dbdb2174d8c51b010f2f8d73a85a8595138f02c4082a27c5348a476794
   56d9e350f3fb7498d84e1b9d4f5171b1c5d238eab7d7c18cbb6829ab9a441be65
   bb4e9bf67147573bee5e5a5bb9b50efac2880bd281b99eaff7e681acdbbe42910
   674884de84f4d120f7a17f0088405174e08d08776f13836d8a646436534663028
   65d722

   // Test vector 5:
   skS:
   c113b4d6182fd5a7918b8cfc938692364ad310f56f0b0a448e07c915e2c88c0c
   pkS:
   4c6859406c73339ed11059cb203e95aed9de0d29a8232bc09a02d0e6c0aeb934
   token_challenge: 0005000e6973737565722e6578616d706c65208278149d30
   94c9138347d7a2bcbf1188a262a10b1a5696c41549eabed84c129d0000
   nonce:
```

```
   d8af21d3f0f186c2219f00d408df3fdec225b3a385b05a14d074270e76db6adb
   blind:
   607253ecc7635b7d308af78dc139bf8e50c5267836d62ec1dc45078d8401b90c
   token_request: 0005576afdd999a852d2b692a0112ffaff3b52188526659343
   dd29edbf15ffa3a30940
   token_response: 8cfd757a54027713c8d0726403d85d7870826d9eaadfb3320
   e5464e446c4442b1dd74493d28f594e240a705c69ada8edad32e3ea0afb8ae214
   e31ccaebabde0602782c0e3a3960f0c6ff008fe32e511a5ecedd9b073d769f0c6
   9cc6be5197509
   token: 0005d8af21d3f0f186c2219f00d408df3fdec225b3a385b05a14d07427
   0e76db6adb76ee4d34d93248d8759177310d19ff8690ccc42f86793cdac069846
   6c3c70da435ab57a2874d19f43300be9f3b86b9862af2dbf5c08c0e2103b9f8a9
   5ded2157acfc7a194756803d5b8e183bfeff8ebe723f89db36b2647730efeed7a
   f2f2130394d57349fd2c9cb13efb9b59160c73b2ee005aaad76ddc0a7d93112b0
   9fdeda

   // Test vector 6:
   skS:
   0b52bee01606bb873f3659b220bedf6d8a796e191e0879c22d0667fe0fe2db0d
   pkS:
   46a454edf9beab6d688dd5e3b5a12ebfd0f05057eaa07198cb59d8d77090e970
   token_challenge: 0005000b497373756572204e616d6520152f7d5c268f3e27
   82afe1bd8cb5fedd71fd63148f629aafec159475876b65fb0005612c622c63
   nonce:
   9558a6deb372d9028cf207997e3ec07698f7acf4015c5bcc8e750da5127927fd
   blind:
   6ae499850850845939dbb3c8777d15bd01ffeda38ba8c6530cde4b4a80ec9a0f
   token_request: 00053aa6d0b8af416e2848e26fc07ec0969362944e7f7635dd
   bb2fc95c48abbf6d0961
   token_response: c8b7904959477a8845c27d9028d78c9a20485b5f2c3af091e
   7831f63a3ea0418f65ba122c97f6a999f9efa3685eaf94a10297bc31bd73566fc
   6eacf7e51c0f085c5f0e20ec6edc0d4ec162b5bab19dedb1bc3888b483b664d7e
   5cc084e1b2b08
   token: 00059558a6deb372d9028cf207997e3ec07698f7acf4015c5bcc8e750d
   a5127927fd90ce141c3793e0d80e94fbb79493144aeea28a1c99dbcfa29443f35
   5f8c4059050682a941d571317fd1b8f5c45d8927e35dcbf4d0c83c7caabd0168b
   ee66083a4028260f80b850bfbe6255ac45ee2131ffecf807789a1baf999232fdc
   431f2ea0a834b4fea79b5c859cc36b991e5dd038d8905677a9275c3fa13d853b6
   e546b9

   // Test vector 7:
   skS:
   89b33741579a50c0ca3ed6a10173aa2104c7f15aeade355eca70532d33e8ce0f
   pkS:
   3c512af0aed3b1bcf06cc960dc8a01a3b82b49851656a07c62afed245137711f
   token_challenge: 0005000b497373756572204e616d6520fffbb92c0d294ce7
   70961273017fe928deaa4a3d6a68572cf47822b1c06da0fc0005612c622c63
   nonce:
```

```
   4de0f814cfd5a07bdb8dce302a62f10e4f0ec642dd7aaeac3d5695876aed28e7
   blind:
   141c6c01876170f6ce2438cf61298c7b47231f49e810c786c7d8b80d7214ff00
   token_request: 0005d950cf438660b794ab27ac0dda4e6e3a6c6f636a91ab30
   028aa5bf56c57c76fc01
   token_response: 8cf6de6a0db0477fad0f53d6d4830bc83baa48c316536aaeb
   709940af129360155620a67d59c5d0325f6fe6c80f981b68eb4fdacaf03f280cd
   58d238e0cdae035f626db1686e067bf71a5ec57b28524e29ef43566e0d6234090
   7a517c1449008
   token: 00054de0f814cfd5a07bdb8dce302a62f10e4f0ec642dd7aaeac3d5695
   876aed28e728e7ff011ffa8bfb9de3e9988ee658468c5ea71a782b0a19151c293
   1386d985c3994d7c7ca66670f7216a63f33ef207d109be93f22931be749d5bf60
   bae00ed9c84827127118a32d35f796f0a9da4e572f8f285cb89c087bc2d096568
   d933ece24440a9a83cc0a0bbd18558c6e3f7b95a14f7b1a48477b15f3f6f8f7aa
   a8b207

   // Test vector 8:
   skS:
   36b4ef4f7a058008d0e6a7c58caee618c8cece7938b02a1a3e0c358a52929909
   pkS:
   4826b0952527afb56f3f413ddc08ee36cfc8432ea96e1430f73317f85cd2a016
   token_challenge: 0005000b497373756572204e616d65000005612c622c63
   nonce:
   9c527eed31a94d8ba30bbce96d21cb509e15ec9fb476445a71d24109bcb9fbb4
   blind:
   13987995de579c6ebd0b342bd471973eaecff20f17aef43e7da41b0aa2ae6800
   token_request: 000555003bfa2896dd98ca70c7f4c3f8ca7742551dc14f4a32
   cb55a6df94a3f4ca2f08
   token_response: 32a1744ac3e0930c1990049a8b3dcef91086183ef68706f0e
   d51eb21f2842e62301f444f2fc20e9090d7d0d6ac4e0ca382f51ef9cb269ee79c
   dcf67643ac9d0127248b43dbf6d2dd04bcbf8df3650dea73219fd3fb3c5e3c915
   8e87b2a6e8d05
   token: 00059c527eed31a94d8ba30bbce96d21cb509e15ec9fb476445a71d241
   09bcb9fbb405bebf3881b04fbb652613bd335710fce992e473ae4c5d860066d5f
   15535bcd1a68d26e07550e8a291e69efedf4265e6917c2dbf300fa8e4ba52a780
   59d60b55421c5f6041507a7da0f81a38065df7b8e9d924c8a6dd1871add0f10a7
   ca3a04049baec89a325795143b5e433af21ed4ca5b737c0c7203ebb9427bdd7bd
   73cdd6

   // Test vector 9:
   skS:
   701e295fd5029617371bc3ac4faa7d2c2bb647968ba34d566f4354166982bf02
   pkS:
   de4d50871abce9e1b57032a000bd21e3070faf625beb1f9cce6f5b9aa4cec51c
   token_challenge: 0005000b497373756572204e616d65207155d0bd2647b8be
   3a23cc7dd3953d26bfc9a6853f090ded0ef64cb9cca93d560005612c622c63
   nonce:
   b6adc3a36190bca49444b59577860f9f864e1aa4a7aeda5a9ce3526577362c49
```

```
blind:
ca73930131684a2babbf620fe09e6a934793372c9c741537c3400c6a7c11110f
token_request: 0005a33220003093091692ad22fcd51a387300eb793563643d
ab8502c32a8b173fd947
token_response: b0075c499f42fa8165bf8e41de97e0277a17e9a850011329f
d6358fdaf44964e579a741312b9f8e68254226a623c5eb68973e019005a15a547
bccae1a471fa0087bb26fb8a5c7c7ed6051ef7e733012736a498c4db5272d7eba
2776e43e2b30a
token: 0005b6adc3a36190bca49444b59577860f9f864e1aa4a7aeda5a9ce352
6577362c495b62fc0a15bc5ec774ca8fc347798f19574c6e90df5c4686eabefbf
2327c2432b77b1e5e8f7ae641c6b216efcaeef85afc8818a90dd8e2e1a1696be7
6c716ca3726283f6a85aa96974b3c13312d82cebe4cc54998851dce409ee10517
12f1a3c7f7a0aa8ccdd090b80d2783de4a42f6805107a9339431fe04aaaaed4ed
52e48a

// Test vector 10:
skS:
c7b5f875284484843602027071f1d1e017b2affa11c9827c3983ffbc4373473e00
pkS:
1ca72bdfd657985b44afb8f79ceda220916f37a567afd0c5943b6eeda40e5203
token_challenge: 0005000b497373756572204e616d6520e5850b1428e29907
00d074cf6907cefa2dfe8126b91f6403f1412dc89640f3a50005612c622c63
nonce:
5b5f7bd44239c9e3501468fb7f8fb9915ec0734429a8f71fe03d39a5e4f4293a
blind:
f2803bcf58776ea00dca81e6279c5292ddf396977ae63188ad5beff405140f0f
token_request: 00058272861ee9d184ab674ed54525a3b0ae1f2d9df41d6dcb
742ec4a4ebc0e0f5087c
token_response: fa074701c0f023e6637e1467f955d11209e65bcbdb8d25b16
db7c8ddf8c7025fbdcb7a471f1657ce0abb0f2be50cc79ab3a7ed37043b4bcb2b
443d2e4290f10de96e9e7daf30b293d4872b0280d488256e7689d3b1fbf0e1ea1
e47762f763504
token: 00055b5f7bd44239c9e3501468fb7f8fb9915ec0734429a8f71fe03d39
a5e4f4293ada9fb87f5409504de46bdce952f2ceca19bd6d354007fcdf043506f
5e3288d1e7abc4b6addf26139a05275fe0594375d059df746a75211be85ff7754
252dfe82ee6403733961414f6818eac608c70b48975ee5e571e1b7d6019aeabb2
cb7133a0b72fdf912089bf66a977f97c88badb9976f0e20a7c138f991cf4963d2
0e1768
```

A.2. Amortized Privately Verifiable Token Issuance - VOPRF (P-384, SHA-384)

The test vector below lists the following values:

* skS: The Issuer Private Key, serialized using SerializeScalar from Section 2.1 of [OPRF] and represented as a hexadecimal string.

* pkS: The Issuer Public Key, serialized according to the encoding in Section 8.2.1 of [RFC9578].

* token_challenge: A randomly generated TokenChallenge structure, represented as a hexadecimal string.

* nonces: An array of 32-byte client nonces generated according to Section 5.1, represented as a hexadecimal string.

* blinds: An array of blinds used when computing the OPRF blinded message, serialized using SerializeScalar from Section 2.1 of [OPRF] and represented as a hexadecimal string.

* token_request: The AmortizedBatchTokenRequest message constructed according to Section 5.1, represented as a hexadecimal string.

* token_response: The BatchedTokenResponse message constructed according to Section 5.2, represented as a hexadecimal string.

* tokens: An array of output Tokens from the protocol, represented as a hexadecimal string.

```
// Test vector 1:
skS: 16e66b97d6e2595c7c7bae5de140249d614ee3445b51f7519a8fe2a7c313
031fef8ed1e15a614234561a4e43595c6126
pkS: 0244b47e6ae241020bfa4ec2fbabbad14c4a3e3dc43a796297121734089b
70020759358b0a093e1b1ba3f8c4587741eb33
token_challenge: 0001000e6973737565722e6578616d706c65205de58a52fc
daef25ca3f65448d04e040fb1924e8264acfccfc6c5ad451d582b3000e6f72696
7696e2e6578616d706c65
nonces:
  - 17a45811bae8ef4a3760e797f28fdefc5c505037411f2267f162faf8d0cc4
  1bd
  - b2b631f29cce6e572c304046d064499db541adc6c300084e8d9a0a7530bd7
  01a
  - 2663bff99c32a5ca5faa21ccf0c5dea29dd33748694846296d94648b41802
  db1
blinds:
  - a1280097a2487cf90c2bf005ff6e4a7f31375dfb9fee6239f73b721edccce
  748b80dc6fe86da39701f2e6d3319fba297
  - d9ee73a1a1e231898f8b9a2e388baf1b7c421f8813b7bcf2b8cae0fb4b18a
  e3e3a0722300c79bd2e90d7158954730be8
  - 9fc032fbaff9369fd5be37165f52394c59f4844567f77cb8d535d9e22488e
  6728694b11e33ce14e7cffa57c737b3a60a
token_request: 0001b840930262d785d05fd837d024775c659020a4872ca6ee
56c13cbe15dadeec12e77cd5a32904e470bb0ca51f6f5611aa2900fd300226b2e
e166aa5e2ec175ed24d9671572ad330a6648b781326e5951807bf56da95f7f7d5
d6a1cedf5b58c3bc340917de6103766cf2d6a1b53b83a33089badfea3df0c4951
```

```
   f488a60f014f2a5e2d0c8a678f6d56f6507e4b647f39a742f1981a393db
   token_response: 409302b94eed3e49b41609bfdccd700894cf559dc642f4b33
   97afe4a5124b2196acaae8514f24db9dd40b3ca4a5ddbb51f741202f72ade5e5c
   bd3917e17ecd9dbdbb0aaab57a637daa4c01193a93c8a28731222a182090b5ff5
   183f893d57e1e9782b51803d0ec40dfac4e3f5c4855810026680a12a2cb008858
   b5682f5e879de543e31dfb12febf8a430a68f5a25599768ec94930e8bbf80b4ba
   300527ce450bdeb98f4634e9caf368a10373f3eabe01fcfd75102c85731902062
   826852531964f215fc55aa0e3be32b08d7baae7134be5d92b1047b277d8ff7cb4
   f146c71a8c1b025ebaba510b634cd9f3035421cd00eced42d2f
   tokens:
     - 000117a45811bae8ef4a3760e797f28fdefc5c505037411f2267f162faf8d
     0cc41bd501370b494089dc462802af545e63809581ee6ef57890a12105c2836
     8169514bce724a0a821c7294180eed5785e946e9f854e4ca3de7e6cfbf2588e
     08cabedb8a302aadff0a21aa348087e5290a305ee8e04a451bf73aab8b27ac4
     ac3761da0149064a932562c06d4054cddd850eaa85
     - 0001b2b631f29cce6e572c304046d064499db541adc6c300084e8d9a0a753
     0bd701a501370b494089dc462802af545e63809581ee6ef57890a12105c2836
     8169514bce724a0a821c7294180eed5785e946e9f854e4ca3de7e6cfbf2588e
     08cabedb8535392a7b69b6834d0cd9ce3ba99cc0424a652cbc91248815377bb
     5c71c1786243879595e312364690beda0ad2f77080
     - 00012663bff99c32a5ca5faa21ccf0c5dea29dd33748694846296d94648b4
     1802db1501370b494089dc462802af545e63809581ee6ef57890a12105c2836
     8169514bce724a0a821c7294180eed5785e946e9f854e4ca3de7e6cfbf2588e
     08cabedb8d25f38c6b1ca8007b7d08462b93ebbacc740a56800b9c762bc032e
     082931956165f190f88567b5ce710af993bf7d4ebc

   // Test vector 2:
   skS: afe6fea6d6c21f9fc6986d2f6e138cea6edf61d332784415500c4fdfc2b8
   48d9250e547d78d1e3ad4bb30938f7fd8b4c
   pkS: 030ca71e4322481a968cc6cf7ef9017df93dc01defba57bd9af3a86705e3
   a66759cffadaa58130b5a1eec3834ee923fb18
   token_challenge: 0001000e6973737565722e6578616d706c6500000e6f7269
   67696e2e6578616d706c65
   nonces:
     - f86364dac08de021f8454d22f76cb2e397db469d1e04e0e0fce1956bb29a1
     281
     - f41cda22fc5503294c23e9008183397c42257299c418e1d2a91d44cad1d00
     aec
     - 57dbea8d2f4b0eebdf65526d18f5b328ca3d84c432b55d428400efaf2180d
     7ee
   blinds:
     - f8a263582248dfe7f5be7dd66a1bf3db822700f65a9b0d3f48ae5171085ab
     50ccc2a41b72466b39756f4dd8771975b67
     - e477da7ee3b5246c0e4326da9a1bac457bb128830681502343eb13ad20667
     dbe68ff1169900e66eb549780e258553767
     - 52620b4bf7f405830d5b45fdca7bfce51cd0486e282bea392d3e748279524
     edc77820f0a7b1f702768cdf8a7b2d4e4a8
   token_request: 0001434093024cf79aabe62a93e92a00c9e7206baab3b11c06
```

```
   11071788e2a2c3f7573696984f9046f55122b2fbf9302c2af2ed8aa50f0284d82
   d9c9fe3fcbe0c9de967bf668ddf09ee3cb9d9f0c86339fd4642b6034bdaf1d276
   7fa649cb495bd51b9482178d4a024e71cee46ffaf6ab26fddd23a8af18752910f
   b73aff9a4ccc912574950386f5b88d2ba98b150c83a9aa46b6d4ed966ae
   token_response: 409303ea334e7bb900a1f91b0eced551946082179fd530949
   b8e2d9746b2e7301c50862bdd0234a1c88c665639e4c0a2a9bb24031dcc4b7395
   2506d100151634376ccd958ca811459f5eb7ba05e401a1264c63c95fd3ff99b57
   7d1ad6eabf2ef0509a7300374e9e2b4bf10c0b82bd6415c945e52343f544e879c
   25e345b6dddc760bfd0bbaa0361c24d7f98d73967db9597c1736462440f1e5261
   c0785f59e1166855b817ea30615f5fd2a4fd6bafc4ac813efa1846dec0f160392
   966797b8bb913374a32e83cb57a77d289c3edcc189d0523e307bfe4ecb6e09b0a
   74d8361859aec9202f9551be379c9bc32e1f696219d87f6195c
   tokens:
     - 0001f86364dac08de021f8454d22f76cb2e397db469d1e04e0e0fce1956bb
     29a1281c994f7d5cdc2fb970b13d4e8eb6e6d8f9dcdaa65851fb091025dfe13
     4bd5a62a8700efdbdce3a004c24dab7b030094b79c5f153c6005de0e74d9b11
     d07d1b0433c083e4d30045e8b692aaaef9cd6cd478a2f360ff253a361a7cc7f
     85cc901624ba902ed2dc0e4493d78167d53cf75a64
     - 0001f41cda22fc5503294c23e9008183397c42257299c418e1d2a91d44cad
     1d00aecc994f7d5cdc2fb970b13d4e8eb6e6d8f9dcdaa65851fb091025dfe13
     4bd5a62a8700efdbdce3a004c24dab7b030094b79c5f153c6005de0e74d9b11
     d07d1b043d4fc47ca614f0c5db31c770de014fb42e3fec98bed5fdaa097b34c
     357076f6b7ffded0624e3632519c816a516c753181
     - 000157dbea8d2f4b0eebdf65526d18f5b328ca3d84c432b55d428400efaf2
     180d7eec994f7d5cdc2fb970b13d4e8eb6e6d8f9dcdaa65851fb091025dfe13
     4bd5a62a8700efdbdce3a004c24dab7b030094b79c5f153c6005de0e74d9b11
     d07d1b04330927c142237a85faf350ea61e176903f58d6c1912a36b33940f79
     2f1ecb99084758ff4b703357f093fcec8d8e619b7e

   // Test vector 3:
   skS: e94b1dd394dddcc64944cc7319f6a2631175db43abf15fb1a6ae4f8fc6cf
   8c1cf6b3385df511601620a2a67c3ecb6f8b
   pkS: 03d4543fe9c7bf8481a15be8c46f1e45be21e67be9c988ebc5e17e794a0e
   8bd6a3e9ad0af978cf045f873def1aa69bf651
   token_challenge: 0001000e6973737565722e6578616d706c65000017666f6f
   2e6578616d706c652c6261722e6578616d706c65
   nonces:
     - 03bf556ce55e4bf9b228fd8849e0bdf274975b360654a2b1996c2be536853
     f22
     - 09ec15b069bdceea683bb40a23c156a0e31e3d6cb2d9832dcee033374e8cc
     a57
     - d5a7df0f9ceda715c8e961a013efe99ac88f12479043551e4e015aab1d32e
     bf7
   blinds:
     - 1cf2f0ffea2df2fbd375c819c8f3069f74424a7ef0a2db5b362f41a9b2930
     97f356cb8009f3619f88b4c65182c83fd4c
     - 2e4d20ebf54e595a72c427c4d06df24d6f68824220e4a6db3642613027daa
     d82237648823dc23e5ad2a96006072bfea7
```

```
    - 7bc11a6f8193ae37629c11e38565efd320ef516688a1fca32c6d48f9be7a0
      77e570ab8a15b3d37b7ef396fd31e75064c
  token_request: 000115409302fad381dd1d611cf7fabacefc59936cc722830f
  f6664754159ee236faa0ea2b9874a670eede1d2ef395557500e7064b6c02c6648
  d0f8ce0ef455b6d12325727ea5f92ed40a29153a4bcddf459cbf90ff9be31bfdd
  8e1471245e0d6fd1dbc09d0f9f033d81c708f8f0957dda5b7949266dff8c1267e
  8ef93a83e574a959ff6c33e152f1833355f90279561efc021f988c2bbec
  token_response: 409302c7a1b7f405585bccb1949da89b607e0d4851d7b8a0b
  f1eb2244d778a1e6031b95d56595ebb247cf3e18d4e212fedf22b03daa80b5b1f
  56d29ad82ccec5de24d66ac7de8eca2bf80b145399386b838ac8bf0e9987ded7a
  fad94c002c4695294dc4402b748b04ad6e0115c672e274161f19258877906556c
  a57d9669a879f4808cdc8bb6c9df1e97ba0e0ee39b31766588bf0ea1d61415847
  f959064fcd9f54abb269945ca42c3548ba94b7ce12fb2c7c26889d2b87f83003b
  43a2489a64c1981b673b49a464b226026b4bf04ffc91d19913536f324683f4363
  07a0d12fe4b32afee2dc61b036325bb39d3b690f0694d78fa52
  tokens:
    - 000103bf556ce55e4bf9b228fd8849e0bdf274975b360654a2b1996c2be53
    6853f221949fd455872478ba87e2e6c513c3261cddbe57220581245e4c9c911
    dd1c0bb83233a0ff77c5d21b63fb3b018ecc4b5416ce4f081b5115456c43f2b
    d59dde1157e630427c081738078ba67f791af80fbd21c6c8342dfc90e39825e
    7ee85130cc2e29a977ff830b080dcf64865a8fd867
    - 000109ec15b069bdceea683bb40a23c156a0e31e3d6cb2d9832dcee033374
    e8cca571949fd455872478ba87e2e6c513c3261cddbe57220581245e4c9c911
    dd1c0bb83233a0ff77c5d21b63fb3b018ecc4b5416ce4f081b5115456c43f2b
    d59dde1152adc03e35079112c47a664658293e13912268b30e1afb89f12e01d
    ffc0dc0050cfe60ef20b91d2c5af85e1354213f198
    - 0001d5a7df0f9ceda715c8e961a013efe99ac88f12479043551e4e015aab1
    d32ebf71949fd455872478ba87e2e6c513c3261cddbe57220581245e4c9c911
    dd1c0bb83233a0ff77c5d21b63fb3b018ecc4b5416ce4f081b5115456c43f2b
    d59dde115ecd05168dadf2deb5156106c2f35a6b55d26f4ff20f756c94c5e5d
    958e6d54e44271785d44c7805ea101f94a36e83a46

  // Test vector 4:
  skS: 2d7c99b16084ee5ddd739e7e0d68ef104e5c1ad7b01f7a221d3356990c0f
  ff87b5b95c64cdcd30838ea5f2ff15090270
  pkS: 03934b1ad9b27aa7e9a7c917941849750db8342922c87a60b8a081768220
  e74a0157ca36582bfcc11eb84f455809ed4a23
  token_challenge: 0001000e6973737565722e6578616d706c65000000
  nonces:
    - 76d9571cf508a54ad6a6ea8c477d9ef54b8795456fb8c2737bfd0554406fe
    5e8
    - 0ecd34d2b1944d408d34b4ad8edb45047b5e412aa254c9f3dcbfa4a4082b9
    cdb
    - c4b6fd80945b9615ca88ba33ad4bf39d6063857c2e70fa091a30f0e96e7ac
    983
  blinds:
    - bdb000ff394d1d7c9076284f10203a3868974c1cb9cf08ea08818b7683a4e
    bd38d67197683205c540b8a8e9e3216351d
```

```
    - 9bfcd6c889e9b0b54b3f8cbf78076fc5dc0eb3d294cc9a30613f4693dc37a
      523c05bd3daf3526a6cc65aa0acb6137d4f
    - 11627c3d68b963f0a233838cffe9e5440f66ba77cd06e7db9e7e38a824fa4
      fe569c9e37cc8fe8b5a10cef8362f6d442a
  token_request: 0001064093033f3341470530709045702 9db7f26f71c04cae7
  25e872c05aea3f243e5506f516c79688f098657fe913c0fd68903b407e0392e55
  b5e08e9cc6ae9188ed1e93bbdbba71773aa72a3112f00551be440c11cf1984d60
  7ffbf8e5b0bca3d4c3f9d3b473031c74bff5c2b0e508e1da6562f44e82e3fb74a
  4e23cae76721ce92626d64be4dfada25f4d7c39e870edcbdd23632123a2
  token_response: 409303f982b51f6c99ea124bdc3b28fd4eae5e9d8659f45a9
  7242c2cc4eee9dd580a2dfdf2b9adabb41b974e3bc266967ef19e02a5630b001f
  e004a3c267152432c3d636134bdf647d06fee05734a6394c6a593645e762f9f87
  cc099b4f20e64dc46568d02fe22e17a5a01807c8cb2b87ed22fdbb38feaeb0b37
  d0f87b5f92e69d2781dcdc2475c18322ae926c2bdc270bee2cb26916f1290eef6
  8be1578c5061549fdd0fa273c44442cd06536d2350f70d3996608268215a83755
  162e1400a1bebb840c301662a6e3df1e74336b6bb8e08fb3dbf5a603cdecba425
  6cffc5295bb37db9769b40c8120dac7bfe37fb0c2ce9af53b85
  tokens:
    - 000176d9571cf508a54ad6a6ea8c477d9ef54b8795456fb8c2737bfd05544
    06fe5e8085cb06952044c7655b412ab7d484c97b97c48c79c568140b8d49a02
    ca47a9cf5bcae9c2bff21fcb91cc8bc0f1d5c31697946de8eb005be5e10f1da
    70fdfab069d2e03d3ffcacb7ac8bef87ef2f44cfaf4daeeea960a465f100a66
    dd9bdfd09e45ed97ef658960af7f39a52264beca7e
    - 00010ecd34d2b1944d408d34b4ad8edb45047b5e412aa254c9f3dcbfa4a40
    82b9cdb085cb06952044c7655b412ab7d484c97b97c48c79c568140b8d49a02
    ca47a9cf5bcae9c2bff21fcb91cc8bc0f1d5c31697946de8eb005be5e10f1da
    70fdfab068b315b225423613928c321f409697ab52d9a457740c834b8aa3837
    ac86351633e96ede8dc655c86dbec920d6a8795201
    - 0001c4b6fd80945b9615ca88ba33ad4bf39d6063857c2e70fa091a30f0e96
    e7ac983085cb06952044c7655b412ab7d484c97b97c48c79c568140b8d49a02
    ca47a9cf5bcae9c2bff21fcb91cc8bc0f1d5c31697946de8eb005be5e10f1da
    70fdfab06efaa503383aed6feeca1e51820d3deb38cf24c6d0586ca34f852e6
    8ee8b7f31065eaa1de7a00ee43c03020c575f68fe4

  // Test vector 5:
  skS: f5c71d296e046ede287571dfd75114dbfe524e7257f4a005fc4d0ebcc33b
  c0069affef99bb2ae601874718ca59de179a
  pkS: 03eab8190ec64355abf0696539c0b86f68e50fb5dc73f4199d5a7952bf1c
  a58186fa4b0dd56368856e21c58df744317d02
  token_challenge: 0001000e6973737565722e6578616d706c65205de58a52fc
  daef25ca3f65448d04e040fb1924e8264acfccfc6c5ad451d582b30000
  nonces:
    - 2a83f6f1d72773dadf94974ebca27d64f5a7f469f96104d82e755369ddc2f
    2e4
    - e76c335f6acb4691d2ba332ba7a40f3819039555779ea66de6f6c739358c2
    772
    - a66b3ce5aeb75777a5178ac561b276240ce58406d6290a26e98786ec0e2ba
    5b7
```

```
   blinds:
     - 4315e207308e508b5b9981f035e77e46c9d45b2f1c0bc45f0d892ef75e105
     b15df7c8813d4044cc61c8ec0463c2641c1
     - 461636f21f7822dacf01631562f4d16df31f6acd0a670d2e3b6506a0e25e3
     8dfd75d335db5d2868eaed9bd060c4036eb
     - 7b8a01654e0f8ad818e3a4e510c8dd5b5a115a0f2f03f1089d90512ffec2e
     bdac9a285c26ac598f17783feacd0eab8d0
   token_request: 000161409303ed7c83c83e9576e6b8ad80339466f05bfd0de9
   09670841a16a3abce1bd382deb05ce0e41680c0ccafae9467902d2bad8028b488
   4dd62baea1659b53049236f64745d086521a53259619b66ac62b1e7e64e54ea80
   3133023c66dc1f3103903cdb520221998caf5f95b9f1c87887672795b05278b2e
   9c4828c532ca31668c80e6835a4de3fa09431d3e076826172ab0a232888
   token_response: 409302429ae37954a49247504c79a77c040f05fcb1825c2e5
   cb25419319211ce1832ee4341f06cc2d44b1580e1e98040ed225402dd2bc61660
   84134a140109edce72ef74f87b14e6a0bf14a81809bb9e7aa9754d254a224c3a3
   aed22b5c2ff234a2035dd03b9afc0b48adfdd8d9600995c95b5bd8c468d546a09
   2c4ff6b3198a0b77b137b52a4655ddd1555a9f19ffe90a8c9fa152e617ca3fbc2
   52157c274292026367de0cf81f2e9ec31a00e47d6e12503a2845eecc26196530e
   cdd9c6f22d873e83513deba2f131f0c2ee39cf1f19c390cbf3245ee5f96b8e9b6
   cc2ad704914fcb5775c2823c07c11df3467d0fe8791631a2ec9
   tokens:
     - 00012a83f6f1d72773dadf94974ebca27d64f5a7f469f96104d82e755369d
     dc2f2e4d4380df12a1727f4e2ca1ee0d7abea0d0fb1e9506507a4dd618f9b87
     e79f9f35ee87b759084d891eb599846514ff6b778f8360e8a1db74e2d05aa8c
     088f8036107c24ae81dc5b6228f81345601d20e83c48c12e35c429469430d4d
     5785f72e1a215438c2b380df6bf53c284a1f928d15
     - 0001e76c335f6acb4691d2ba332ba7a40f3819039555779ea66de6f6c7393
     58c2772d4380df12a1727f4e2ca1ee0d7abea0d0fb1e9506507a4dd618f9b87
     e79f9f35ee87b759084d891eb599846514ff6b778f8360e8a1db74e2d05aa8c
     088f803615c8326b73f2c12f07d98a97f4371905e74a3940b8eead7a2e6fc9f
     f3f90c7b24bf938910ca4fb1680b78178bc83845e9
     - 0001a66b3ce5aeb75777a5178ac561b276240ce58406d6290a26e98786ec0
     e2ba5b7d4380df12a1727f4e2ca1ee0d7abea0d0fb1e9506507a4dd618f9b87
     e79f9f35ee87b759084d891eb599846514ff6b778f8360e8a1db74e2d05aa8c
     088f803618619eaaee20d918ecb4b35f879b0ba9791fcfda086e25366a0848b
     dc8940b2ded244b1be025afa8c5403299196cf883f

   // Test vector 6:
   skS: 2795bea1931d9eb18ea8f341f9136d06825bf87900aadd5cba32f7e7501e
   7e05fd867ed88b7148676c4f747fd455012f
   pkS: 03b1144afa40414bafc6d27a46ee314ecd183641c631b6d406b5d0311e7b
   6a64e9dc561223f38913a5fd299ee437275439
   token_challenge: 0001000b497373756572204e616d65000005612c622c63
   nonces:
     - ba1832b01f112d463d35f3df65780a8af5186f5a036b4273f488020e6bcda
     4d7
     - 2feb86d353b8af5e75e8533b1c17cd4c18c387fbe485a044a32a3164deb30
     6df
```

```
    - d9d7d698370bf231c1b81766a750e285a6b860069d826a9d2367f28a79c57
      21a
    - 733225c695c68f2524e364dd63d35bf5db28ac5c3cebf7bffdfc60dd76ed1
      22e
    - 2ca686cc3150f70093c492bccef6b40b34fb273be2ddd4faeaa51f14b1d1c
      3ef
  blinds:
    - 1845b65b595a9f07d737fcf1c9737489c1641bdcc889b9d6262a8f2d977c4
      b5e98ee502fe6e44e606c7bcaf4a2f74b04
    - 123ce70d4ba8c0a3280381dc507f59c8e986e7bc3e71e1adecbbe5f800b93
      72901e651b3e9df66879d47af4d324b49b8
    - 729ce122eada4cae8a9dae5b026daabaebf9a9c2f93cc74b4efabf6c1cce8
      8b593dbe07c1196c2e2c5f83f3f5a11c999
    - 5fe96b7399afb7fc5dfce3911fc586add59838a4130bd1bc9a39da4d3f0f6
      1b2f778bb4b6de05f1e2fafda0d3de48670
    - f815705a65ed835081cf6cec6e72b110e4135bf559eba7cbd8757d90c7dcd
      dc573d75bdc8ad86cf61cc1ae6b6883028c
  token_request: 0001e340f502290ec59ab9063137d3342c5618748059bbec22
  84f4e841a925fea9cfaff565634592e7fa066d0f4d355a4aa2d5b305f10246d9e
  28f9ec550954b22492bbdd21652da7c6ae64a8638757ffb48ba9fcdc46d5e44bf
  2cef90dd20c7c1cfbb203e05d003c2db7deb628339c677c9f8a39ed7cae085028
  4025025ca590ac60d9fa7e5a27d6eda67fd0b8c9ec79dafe3bac404839502a1a5
  ac19a2cd95121c602bd54184e7c8012199f05cbfa1af96d077130a25dc4edb0e5
  5204611e76e2de7815a32f415ab03b7907caefc6d3acba400884ac5763eb022da
  05c134ab19186b4b5b51f41e8b0e8966047c482c50235cf01c5fd435ccf1
  token_response: 40f5037fe5401091c1ec2fa44643227c2026195162e07f794
  92b0f19c13cc2fffbd8e1755f76614fb9bd1ff9c0467d9334d81b0285aed2f5c7
  0a29dbee0c7081dae4ba76b75204b414a70e66e2d17cf7c0a108930182b88222f
  0b1ec1435b10dfb11a780037439fed66b56b8ecb393e1b2293cbd4a86ac141e04
  7f1ad891f28c3f062f339c18318feb889c09c7ee84129bd88aad3e021098e2388
  03cba587204424f89efe83513d8a66ed7f9c488d8ee1b17baf80a5a6e1b3cdcca
  07ae98ada345c28ca01f8103f74cf72200f0aa7d630232587c20c4c70f6bfd963
  6681919777699e63ecc85e8965333341f58cded92b46f30e9033d4e8c055f54ff
  fd89089d8a979fb398b0e3d6de160b0d61bd83759057e642b77abef3b7be4ea42
  4236c1a6d804f1974b1ec194bdfdc78458e252f8a3b08fbe2b18cb3c355b328a0
  1d16cceb9485474854c006a5fab32e1a63cb98c739d761be2e7e
  tokens:
    - 0001ba1832b01f112d463d35f3df65780a8af5186f5a036b4273f488020e6
      bcda4d74d1a8f1a708ab7ec6f9ddfe97074859fdf87737790491e4b3afd0977
      cd3bd3967ac8049affe0727785606abba401320f4da956669c1fd8c3a6b544f
      f9831bde3cbb14b733c723655c93ad2e6c8d8d9a560665360486f1699b4cc1a
      2671334875e76f816a151f532607ee64f55793a6a5
    - 00012feb86d353b8af5e75e8533b1c17cd4c18c387fbe485a044a32a3164d
      eb306df4d1a8f1a708ab7ec6f9ddfe97074859fdf87737790491e4b3afd0977
      cd3bd3967ac8049affe0727785606abba401320f4da956669c1fd8c3a6b544f
      f9831bde3e77d754efb404a1d034b4b6b1a8fc1520e8105f2cc4dd13465bc11
      7b57ee2d256b69362407164d66cd4ffb91b46624e9
    - 0001d9d7d698370bf231c1b81766a750e285a6b860069d826a9d2367f28a7
```

```
      9c5721a4d1a8f1a708ab7ec6f9ddfe97074859fdf87737790491e4b3afd0977
      cd3bd3967ac8049affe0727785606abba401320f4da956669c1fd8c3a6b544f
      f9831bde372afc55fb181d380ca3cb818466408427fffbc89094d2dcf282353
      f3f64a8cda8bfdc7918585a15683d3b40905f2f720
      - 0001733225c695c68f2524e364dd63d35bf5db28ac5c3cebf7bffdfc60dd7
      6ed122e4d1a8f1a708ab7ec6f9ddfe97074859fdf87737790491e4b3afd0977
      cd3bd3967ac8049affe0727785606abba401320f4da956669c1fd8c3a6b544f
      f9831bde3054b234a476ad24ccc82fc8be0515b3be455fa831b849cdcfef243
      1c02880a27b6d7599fe93d7985db25262f3f0d5e3f
      - 00012ca686cc3150f70093c492bccef6b40b34fb273be2ddd4faeaa51f14b
      1d1c3ef4d1a8f1a708ab7ec6f9ddfe97074859fdf87737790491e4b3afd0977
      cd3bd3967ac8049affe0727785606abba401320f4da956669c1fd8c3a6b544f
      f9831bde3c9488481ad751c6e0e124d5b3da0f7386806e5beaed1fd31cf6e9a
      4954f0708e1c3a724d40077edb0f4a12975d35819c

   // Test vector 7:
   skS: 00b22fc44750a0be95910b42350cf889428b29822137ae7c947dbbce1211
   2252955eaa044c2d1bf04d7828a2c1a607f3
   pkS: 03fe7d3412c17f4d9c95fd4b6664f980903de4ee3e33e4349cf6be53eb0f
   e5168aa9ba53388646cbbcf9742d63ec6d3ec3
   token_challenge: 0001000b497373756572204e616d6520eb86d4628882f211
   a5a9901ef73bfc808681f803935eb278cc6741b67346d6520005612c622c63
   nonces:
     - 777a3fd1afcc8fe4e2b69bad782aec122f7517530d5ffa813d2322b12165b
     0dd
     - 7248c86afc2560aac6ae6725026f5dc2c7177c3d1bd9fb90eca9537b8f47f
     352
     - 85f92c1d25208e349270deb3ebab68eb479befdab76a847943e80c98a6480
     2cf
     - 09dd90d14e95a707be4b4b0ac91f11eb2ae87573000996a824e7b53fd7f8e
     b49
     - 7e7a5d87ae34c8f754baed42aff353ce54121441f6673e173324116e24d45
     d07
   blinds:
     - 0c413fc7b0ba7a07786863406b814afe49f98bef60dd6f4d94a322b5fc3b5
     fff0a67e147f427947b8c2d69d7a1a98d72
     - 781478668ad9c06716addf134d89d8c5b67a7402db8c35c52cf62858519e6
     fa95232efd8f2202277263450bd68105db7
     - 70be1eb3a8a03053d713f735b4f2981f8bf5bc0726e1014848af1942f25c0
     f6ec6a4138f6be7d44d093c2cade22951df
     - efb1173321ecc93ccc6a3292f532de3f8229d463dbac9a72ec9960335328f
     088faa7413c8f6f8df6000fcd842a024556
     - ead8b0b7e50cb3e138d49b8f7fd382b9c570b35fbf5afd7ce2441eac797d6
     0c9911da2f964b231d5473d5629adc50932
   token_request: 00014140f5022fa0eae8e4413e1285554348c51a910b685703
   f535260e024efce29ddbd2b6afb661bb46d723ab0047db99b228716908037ac9a
   b495355f8aca5e300c6c8c429a5d6ad7596df529e87ee7873ff67b5bdd5ecee31
   b6a22ee0588bd03148247876bf0361222090acd961ee4c7d0928b4dfadfc95075
```

```
   1ba8129cde0367665719f1da0a576323152954d6cdb49598a9f620a6e3903dfb4
   2521831994cffac87a588e1ffedbf5c5bd617034bddfc3677efa5d95ec9b4dbcb
   91c26ca23b8c03ed431a1bac9e402a71d2ddf43f161b225b8e4f16dafe7fd2b90
   4882e61336a3e461a02595ae602ff2007251a9b3b592a458c75ea5a0b769
   token_response: 40f50243a2a7461641ab15ffb51a55d98bca33b28c75fba03
   f42cadcf4f8d4599b1cb26dd1cd284b03e4d52f9c509d72ccc9a70371df152264
   77fb1cf1a78b93db07b5f7c336ead3133c7fc72919dbe6249e7ce522911e68814
   766ae3255040caa62c5250358fecbda72a5a77a56ab674e6d76b55f2b4c5b9033
   a6f70cb4e56607ca0082d0d5ae82bd96985cd89c81e2acae628672027a50d7bc2
   99756a65bcf708ba92b5d6e9eae44b76ac54344fdbc7e3b3ac7d202f046d96cef
   39c168645132aa31c669fc029ff3e9245c5158c7d2f87450ebd0d743996438aa8
   2205501aa0c1f56d071ff5c3f2e98b09a738ab4f8f216dc3716ae7aa6d1f249f8
   65a2f0b36b52b8f58a66ea985fcb9dcfcaaf3bc92c1ec5d97ed4d6d1c88bb909a
   f64317c2885d140619c959dc6b2b58d8bd6e09fd1b8bba638bf142e282c1ae6ed
   134338cfea2cdfdf1f3265db8203875218b979883cca8216e394
   tokens:
     - 0001777a3fd1afcc8fe4e2b69bad782aec122f7517530d5ffa813d2322b12
     165b0dd35889a45e95bbc66bb8b042482644693997d94cbc50853af61b34275
     6828e81bd5cc36b0ae0c64bba34c5e560ffa2176a4a39fbf8fc57e2befddd20
     d8718e341f7dbfa4a5e5e603dc415eacf0389643f48abf09808fe83ee82ca08
     2ac89c5857ce0b9043aa0ff3382e053a0a6401746c
     - 00017248c86afc2560aac6ae6725026f5dc2c7177c3d1bd9fb90eca9537b8
     f47f35235889a45e95bbc66bb8b042482644693997d94cbc50853af61b34275
     6828e81bd5cc36b0ae0c64bba34c5e560ffa2176a4a39fbf8fc57e2befddd20
     d8718e3415c5326a9a877916183bf8f04652d9df41e717eb4c4673030d4bd88
     bfa3ef0df371cdb2f50ec1a0f994f11bb324b355b2
     - 000185f92c1d25208e349270deb3ebab68eb479befdab76a847943e80c98a
     64802cf35889a45e95bbc66bb8b042482644693997d94cbc50853af61b34275
     6828e81bd5cc36b0ae0c64bba34c5e560ffa2176a4a39fbf8fc57e2befddd20
     d8718e3412965c9aa4d87dc58d91bf7ad2fc0b182d12e1019bbfc5c0875b763
     e2e4a1cebfc903f6c4d9c1e120ca62c0a1d409c1ce
     - 000109dd90d14e95a707be4b4b0ac91f11eb2ae87573000996a824e7b53fd
     7f8eb4935889a45e95bbc66bb8b042482644693997d94cbc50853af61b34275
     6828e81bd5cc36b0ae0c64bba34c5e560ffa2176a4a39fbf8fc57e2befddd20
     d8718e341a0e9642df13a86061747d852d1725508895a4f0c2e7b07057897fa
     d4ca45ecbe6b4b0b7169edd2c6ad33e8cc4041e721
     - 00017e7a5d87ae34c8f754baed42aff353ce54121441f6673e173324116e2
     4d45d0735889a45e95bbc66bb8b042482644693997d94cbc50853af61b34275
     6828e81bd5cc36b0ae0c64bba34c5e560ffa2176a4a39fbf8fc57e2befddd20
     d8718e341e49e1e468df8ebca7f2851a89b377c529b7857145d4c300228c9be
     2f9ba0ff9c97247bdad2a62d8b39daafa8ec7b914d

   // Test vector 8:
   skS: fe9dccf471b18e752daf169864b11d36d52774540d30ea3cfc956a9fa2ac
   356b15e3ca04357276f9f27575aa2264f0e2
   pkS: 03ebbe14213fba10b5961b2ce6005c865ef27d8a10606886e5240fd5793d
   57f1c1d6136d20a20411d667180119dacca915
   token_challenge: 0001000b497373756572204e616d652077c9f82ad689b6fa
```

```
   eb0bf5e3b7bd72c220beeedf1ef15093facfa9685f3c88950005612c622c63
   nonces:
     - dea96b6ebfdbe8b3f228023159e3589e7cffe39fd79be31baebc3dd86fc2b
     f1f
     - df8231412e3f6e568886adfdb0bc270c417260de1f15aea9c20e81d0ad79c
     0c6
     - f9ac7d920db5da9430095b97030bdef8d60c387122a9a239d488fbb9b2331
     536
     - 3caadeac6c38966e745e6c09b6d143fd8361463256de25d54cb056d5df305
     ed6
     - bc9a18f5d8188ed973fa11c346b985437aa3cb8e9cf2395a81a08804c8183
     e09
   blinds:
     - 261310108a900b80dac58206d0131b639d15ff3f44bef4aea760f286f4aff
     fc804366c86e9d5c655310f3c5a4504dbba
     - edeb73cc4d10cd8e53f344c1d9f0d5713ca917a17ab2ced91289c74f6848a
     bbe782b560879d8c1aab1d3a07ed0f59e9f
     - 7675f2b9d18285f0c70f7f3c345e55cf10bf81acbfeaaca984314af421331
     4a6ac324f8db66d8ed541afc797827394cd
     - 7f562368a21814fa3c9c062910cc74128315787af90ab4a74d7bd8750a069
     e1c83edff770f86cf518e28b34a75ccb243
     - d007777c470c5ce0fb2123466ac3139576be4e320e2a61bea4231c793af94
     3281f84439f135536a8923d5aca4b40d0b6
   token_request: 0001e840f503de448f06485e806c46357acc187d1d935886d2
   3061dd2bbefc18bb3abada39029d976a60b6afd7e03037736ff18efef20308fa7
   0011010abac2ac2c2d014fbfa5d786a5954808c42e35038de42d9de3851653d78
   558273ce2fbde0c67948f06719020e9828ffa3a98380b902a85b1e1c94816a8dd
   e721e66ce9c7f75fc36b5c035de03e61e6d8c6778dd6569f8ad7c6ff7bc0325dc
   e1625d45cd0b6a82005cd217aef1352072efe56f73f69508296f3acf62e174c78
   0f691b706af621b64be94ca38080334a147c42ff0dd7388ddaf981e5f5006eed7
   500fd222331def8dadba1e50175294823ccd0c6b73256b57dc6520f01cf3
   token_response: 40f5037e24738ba84969dce153f7e87fe66b3e48409ac4c3c
   1d88d99cb0c624a9a98b707e9e00990ea57916c5bec20e588434a0266311282d5
   f269edb2fc082f34f25f680f091517cc0bfbd7bc0bfa9125a2d74f6081f2ae4e6
   43e8917edc19454d049db038faa3c1093f701db56b2f1f14c422a127de6929b28
   e39ecfd3d8a1d632c9aed8b1728fa820f41f47bef2233a228f5bab0209909285b
   d479fe86c4c027417d826dfdb7636a969a849ddacda503c24de82b90897e7229b
   517fd3f0393ba9e19abb82023e1d5e41a056587748ef896704dcaa7695e80605f
   aafb609b80788fd9899925736b581e6e4837a28725471ae677fd621c8ece95de3
   f1d98fac39823ac2921ec52c7b05cb5d30ab33e0cbcae377fe40c528e23ae8853
   0d852d4928775d8c1f1def572087592ef6176d5790ab8adbe0523328a8e092568
   2347e6ca8fa502bcca05e8ece1ff86f1b50c102de347d08792dd
   tokens:
     - 0001dea96b6ebfdbe8b3f228023159e3589e7cffe39fd79be31baebc3dd86
     fc2bf1f743229db4189b04ef5f90ecd3cf54a2476aab8c026a1f5af81b7d542
     5bc512318924fee28549cdf14f42cf3441cf39759c04f6e6a162a7c61898315
     85de491e892d9133664d98050e02dce92a157306e5d9eeb3a84bbb74d40b05d
     cb3ec286a32d247012198daf729a17f2f76210f4da
```

```
    - 0001df8231412e3f6e568886adfdb0bc270c417260de1f15aea9c20e81d0a
    d79c0c6743229db4189b04ef5f90ecd3cf54a2476aab8c026a1f5af81b7d542
    5bc512318924fee28549cdf14f42cf3441cf39759c04f6e6a162a7c61898315
    85de491e8596e9a710d28167de1aaa8e9bba5ccaba514ca7774a890496441e5
    fbc50ffbc8187c2b9015ae728800d190c48496cd38
    - 0001f9ac7d920db5da9430095b97030bdef8d60c387122a9a239d488fbb9b
    2331536743229db4189b04ef5f90ecd3cf54a2476aab8c026a1f5af81b7d542
    5bc512318924fee28549cdf14f42cf3441cf39759c04f6e6a162a7c61898315
    85de491e8a431c43cab90b664077608e2b34a06ac56c1827a2f6f78b7736848
    0e4517744e8a3e10a690a1b173b745540e68fc4f5d
    - 00013caadeac6c38966e745e6c09b6d143fd8361463256de25d54cb056d5d
    f305ed6743229db4189b04ef5f90ecd3cf54a2476aab8c026a1f5af81b7d542
    5bc512318924fee28549cdf14f42cf3441cf39759c04f6e6a162a7c61898315
    85de491e86ebcab5874aa2a52b7dc764addcfd76839718a13a048fcb8c2abd2
    2c3a7b90fc3f48e38ae21072b01a415af65b36a2b8
    - 0001bc9a18f5d8188ed973fa11c346b985437aa3cb8e9cf2395a81a08804c
    8183e09743229db4189b04ef5f90ecd3cf54a2476aab8c026a1f5af81b7d542
    5bc512318924fee28549cdf14f42cf3441cf39759c04f6e6a162a7c61898315
    85de491e8e7f0f3a47d721b4a408670ffad7b27627421a6be3af7f75068196f
    a26fe53a62c3693b5a1092985795f799c30ca73d72

  // Test vector 9:
  skS: fa1a7f2ccb6651e82aefef530837b518946ca8df30bfb6b629cadccea965
  50a2848b649cee5c91e3dbaf30e62fe6b407
  pkS: 037bd0654b77d1b4ae8d7a4775b04d06f2c406496ff07274f79e956e6ee8
  e6b0668457894b84dd18733017b2fbec89c3f9
  token_challenge: 0001000b497373756572204e616d65000005612c622c63
  nonces:
    - 8bc16d866d0193d20b435d49f58cf869f8c3891e7e6f7bf0cce5c5e29a485
    9fd
    - 3cdf1e2db7a86eb1e75fdbfcac7fc044c29cafa3d40ddc769c0c21f4286ac
    5b9
    - 99e334d0713e797bc836545e0dd7dcdee1993436ef6889b2d615742665740
    8fc
    - 32f356152811342c0b4ab9e34ef16939bc6422bed4e73449b09065f19c057
    364
    - 6cf58474ca44d5f86f22f44da98f15939a97645f4c60e565c2be332800ba5
    44a
  blinds:
    - 85c3c875b12d4578fe905a61fa37cc3a16ee77d87f09705e684833951b692
    993a5bb663427b8dd10915804e091fe5aa2
    - 205c94ad910c602bd3f29404d10ebb89b9148b0ff4adf065ea04f6fc5e240
    64d86bdf7b2e00962cde1d1ab48b42b3ac5
    - 7dbf232de16945358b5ef69b2740940530b651d37708e70735dcfece2e9b2
    18dc82d75a60f6499aa5d0df6c818407405
    - 9c3c5cf1182f26d0fca4c9c1c883ac78aa7b4dbecf560cce8d495a0952b5e
    2377384facac0ccfe30afd3cb50c132fd87
    - 83a0546a413a3dc5dab902dfcc21deb38769cf860288b6bf2971ffa93aace
```

```
    8f4ec8d024eb5962e84fa67967b53bc4201
  token_request: 00017840f503741b71eaf59345fc7f7dc8d7e2f55561ef9053
  4da58150b51b7e5e97cf7bb20d8486b252f162c5feefc4ec52b222751803fcbef
  bb50a51f7c0c28a5f078bb3be47f0f14989ad8a07490ac39423e4d5bdb8e13e40
  ece67295e5fe7d9af6bcb2fe9f034feaf7cd856dbdfaf4517913ae44720e4b184
  48f4f1bee274a56a31fb62de0fe49b280d19212609b41c6ed90c4919ff403e77b
  87842ed6160d1d36ad218fe35d8c6f077e8b48a978ad0373546c0fe4066fad073
  acd2ee25dd22535b2c2fc20dffe029f41b5b88625eb8cd94787bebf272ea5c756
  4ccaadeb1ada97ceda15212c2c4f8efdc00c4fe2e2ad58263a2ccc4c0ed2
  token_response: 40f502e6fad442191944d14d5c8b467b9c0c11ac06b0cdc1f
  3f5a9a2d55974f2f2125e0475e83b50f13620b3a817e1795436d703e76c34d0bc
  d846876ca664ccd97452104c3f7bfc035f3c7c09f0ef6a9b81c9aecb6c8bb58bf
  02edca7bb21590db2bd650225cd40a928588f1511c4603616151f69661393a42c
  3126ff3622187cf7916872b898c633790cf7ce42a126e4413ec593037b2bc3a2c
  135098f7c69315db242693e411838ecddc1cf88d968ed8d72b5611dbbaadb4988
  f0f7c53a936ba39a68f81e028ff4bf6fd737a137adee95d2fb773cfc810251485
  9fa419c5e8866dd64d7c0544ec39793bab6384d1d129085cc8af450c8689751c3
  a15f32c0e950624831c8525614e4e7cf92645e8747d0b1a6c95648bca2d96d20e
  e5b44ca44491787af6382049ee400b719035a7e3fe2dec5f9155e332fe24b5bb8
  071c2f3fd00cab8d2a1dc685f6983d043d6591fe00e2ae5a9f89
  tokens:
    - 00018bc16d866d0193d20b435d49f58cf869f8c3891e7e6f7bf0cce5c5e29
    a4859fd4d1a8f1a708ab7ec6f9ddfe97074859fdf87737790491e4b3afd0977
    cd3bd3969e07ecffb1faa3a20d061c88f1e5292fb4cebefa1311c28eb5f37d4
    75606b278ff35f1fcf8ed7ce3aa10bc2f0f3302d20b0bbc1fa5c45be9d912d9
    7303b9aa8aa0d28dd80d7efb86c9073211f811d93d
    - 00013cdf1e2db7a86eb1e75fdbfcac7fc044c29cafa3d40ddc769c0c21f42
    86ac5b94d1a8f1a708ab7ec6f9ddfe97074859fdf87737790491e4b3afd0977
    cd3bd3969e07ecffb1faa3a20d061c88f1e5292fb4cebefa1311c28eb5f37d4
    75606b27882e60cfc6e7ed2b433bdfdad3d225ed09ad3626f67025a26311608
    0a9ce17142d8565fd9ceba77182757e6202185ca6e
    - 000199e334d0713e797bc836545e0dd7dcdee1993436ef6889b2d61574266
    57408fc4d1a8f1a708ab7ec6f9ddfe97074859fdf87737790491e4b3afd0977
    cd3bd3969e07ecffb1faa3a20d061c88f1e5292fb4cebefa1311c28eb5f37d4
    75606b2788d8095ab268d6715fb89370bfb3c837493039506dd1a3a8d07a63f
    065e8e7cd2e57dc3a210b24b7636c8484273eccc17
    - 000132f356152811342c0b4ab9e34ef16939bc6422bed4e73449b09065f19
    c0573644d1a8f1a708ab7ec6f9ddfe97074859fdf87737790491e4b3afd0977
    cd3bd3969e07ecffb1faa3a20d061c88f1e5292fb4cebefa1311c28eb5f37d4
    75606b278729e03e210cc2486c4f747b5ff67a239767e32f611f6da82a0ff36
    c2dc047e1f48fe920677c4f53c60ae1c735644ac55
    - 00016cf58474ca44d5f86f22f44da98f15939a97645f4c60e565c2be33280
    0ba544a4d1a8f1a708ab7ec6f9ddfe97074859fdf87737790491e4b3afd0977
    cd3bd3969e07ecffb1faa3a20d061c88f1e5292fb4cebefa1311c28eb5f37d4
    75606b278911447f48e89e5d66c5c52e2c0af0729300e69ee6e5e39d465b836
    41058cf4f6460bcb4672fe37de8b0efa1bcdf33c16

  // Test vector 10:
```

```
   skS: 88afd78d73efbd37b94183cc1d6fb8e3a0dfaed2ca7f715d76e44843e3c9
   36a266dc3335cf16a63ef31fb6fb4a81771a
   pkS: 0363010d08ed8eb12d29e6d11059b7a02d6d665d8212ead2f19b43a96a5d
   f6211b2be769f8cc87a730b814cd1013e039e6
   token_challenge: 0001000b497373756572204e616d65000005612c622c63
   nonces:
     - cbb64dbf9e920048a1c5517a8a12b44a294b5ac5ccb3b366178f1031f7c46
     56c
     - 3156fffdf77f4f0dcd23406bb121d3eb18e4d0a8b7286dc7c10bfeb58305f
     e97
     - ad0930ca85e54145cd8e02bc6508a0e9bc525ba9feee3c19ec3d6258e368a
     674
     - a70ecbb14478c7c5af0c5f7a9ca4dfe50c7ebc5ad0c06f1addcd3e406520a
     f23
     - 7ecf841fb195b155fc443f46c504840a0270464d7e10862cf134438049c66
     f7c
   blinds:
     - 421c533dce493799fc44c217d2999e75f1158b256bad86e4f13dc94e0f9ac
     a2dc09ec3ad286cb011d63766a0f0679c0e
     - 480fbbcb53834cddabea02c0bdf2f7d7af1d9fad3f71534cf2cc92818262e
     6c25dfd39a7d69489ba1c110dd97497735d
     - 819d08bbde696e245e7987b7bf5b0cd5bc5e188565a8e3191bf9f11b06462
     6f504e1fe6d5d1c7ebe4e096cdbed79a79f
     - 3341d181e8c09af12a3a653a290c5977607f85ed5e6394d1b52e0f8976808
     1561aa46016b917d9502cc207f10e164a89
     - dcb1b2f72a5f88b4182fb431911468b4f1d1225391900c9d21c2a0ad1b795
     c7801648c4f8e3f88c488d3b6d5109bb72c
   token_request: 0001af40f50201016fa016b79e0ac32a62f05e4b3c05a8a98f
   2a91d3345222e7b45d464530919bdf7e13009d41dc7d80ff968a5749d702c13ce
   880d0198173e4f527fb18999e9920dfb6fefbaa758723b962643bf72d09d4305f
   622757fc54a7a99b718812f91403024b6117c0953f53e1c582b6847288616bc97
   34bbafc4feec7d9b6bde5c768db1cb4e7d2d3abac5e709f861d9e4a0c8b03c05c
   15addd2a8a68caf2630d432ba5fd1d56e458869df8885db54d006a17897919e08
   95b5a570efcadb08b81063ebb830232404a0ef1947bc79773ce4648c35bfbd2e2
   542578fbb0fcdacd9e87c39ed33b36a27678f5746cfc4f94099ca588ee54
   token_response: 40f5032fe65c3e5244e485c42953503b950cb9d481fd559a0
   415593120b164366d51229eab2b0f9c75fc8d56b6a163ac71192b02d5a761c49c
   af9c4b9a0c3019bd1f45a59b8f3d9acaee9af7d0f72e7bb47dc4da80324387a22
   1b0872321188e6410fa0e038fd7f3d7e60caa7cabdc765d8feb463a2f5c7fac60
   63119dac9feb658d7b331657156aee7794ca77e68ed6b2986a55ee02a18cdd372
   c76bc9ff8a9b6ae47324345c515e8114df9392eea70960bb2820370a71c66fae4
   8520ffc475fdbb88993f0c03005755be30a542d4c0861ae1f7ffd584355eecb8b
   2f0277254a6917661ae91a708eb5cb550cce6955fa873e755fede7310d34e5552
   f3d542910c3ed98792d670df9b82731ca82b8e674ca4245f6fb89b95f114e4252
   aa1e477707cb016f39a297b2755043b34bbd1bbc32583e8b240fd0dda4c8a6764
   1992c04f6d56b46b195507b7ee05c3c67004ef9f059a864c7f52
   tokens:
     - 0001cbb64dbf9e920048a1c5517a8a12b44a294b5ac5ccb3b366178f1031f
```

```
      7c4656c4d1a8f1a708ab7ec6f9ddfe97074859fdf87737790491e4b3afd0977
      cd3bd39698517059067b3eb2bd6112ce46b67b6724ae86d1767cf8f171daeb0
      f8bb213afc44c046b33ba4f0f0d404b19bcd73e7c88a4691af2ebb660592df6
      0d6d090abb7711a34c8c78ebd075918f792804e221
      - 00013156fffdf77f4f0dcd23406bb121d3eb18e4d0a8b7286dc7c10bfeb58
      305fe974d1a8f1a708ab7ec6f9ddfe97074859fdf87737790491e4b3afd0977
      cd3bd39698517059067b3eb2bd6112ce46b67b6724ae86d1767cf8f171daeb0
      f8bb213af46c306c3497f96478f6040344d4981665eeef7b8e4cf5ce14da0d1
      f98773bb5a1be37252dc7ec61f814304270640572c
      - 0001ad0930ca85e54145cd8e02bc6508a0e9bc525ba9feee3c19ec3d6258e
      368a6744d1a8f1a708ab7ec6f9ddfe97074859fdf87737790491e4b3afd0977
      cd3bd39698517059067b3eb2bd6112ce46b67b6724ae86d1767cf8f171daeb0
      f8bb213af6823c16eabf6871797ce45c17985ed3c29ff08cb61d53be4fefd4b
      81087590826e679e2cea1cfeffbfcc82993731e5d6
      - 0001a70ecbb14478c7c5af0c5f7a9ca4dfe50c7ebc5ad0c06f1addcd3e406
      520af234d1a8f1a708ab7ec6f9ddfe97074859fdf87737790491e4b3afd0977
      cd3bd39698517059067b3eb2bd6112ce46b67b6724ae86d1767cf8f171daeb0
      f8bb213af60e3e68ada8f217c129fa2eeef3a3c312794eac23f1fb4eb8b12ce
      672b9963443bf1c80583b4150d35b6c16871f10321
      - 00017ecf841fb195b155fc443f46c504840a0270464d7e10862cf13443804
      9c66f7c4d1a8f1a708ab7ec6f9ddfe97074859fdf87737790491e4b3afd0977
      cd3bd39698517059067b3eb2bd6112ce46b67b6724ae86d1767cf8f171daeb0
      f8bb213afbe9b2790151db3683b3ba4865e71aa2b0e6f60c500e30995217e88
      b772caa1f5b26f94e4766872d764656e268c274ce0
```

A.3. Amortized Privately Verifiable Token Batch Issuance - VOPRF (ristretto255, SHA-512)

The test vector below lists the following values:

* skS: The Issuer Private Key, serialized using SerializeScalar from Section 2.1 of [OPRF] and represented as a hexadecimal string.

* pkS: The Issuer Public Key, serialized according to the encoding in Section 8.1.

* token_challenge: A randomly generated TokenChallenge structure, represented as a hexadecimal string.

* nonces: An array of 32-byte client nonces generated according to Section 5.1, represented as a hexadecimal string.

* blinds: An array of blinds used when computing the OPRF blinded message, serialized using SerializeScalar from Section 2.1 of [OPRF] and represented as a hexadecimal string.

* token_request: The AmortizedBatchTokenRequest message constructed according to Section 5.1, represented as a hexadecimal string.

* token_response: The BatchedTokenResponse message constructed according to Section 5.2, represented as a hexadecimal string.

* tokens: An array of output Tokens from the protocol, represented as a hexadecimal string.

```
// Test vector 1:
skS:
91f04a2caea9a854cd351b68d58132a6afa65d4dbee00fd55715d553d744820e
pkS:
909b2a8c70e4f70c4acafc87f027d41fb1ac59f7ed62845a8ef5cda4300b5e2c
token_challenge: 0005000e6973737565722e6578616d706c65208278149d30
94c9138347d7a2bcbf1188a262a10b1a5696c41549eabed84c129d000e6f72696
7696e2e6578616d706c65
nonces:
  - 62dd654dffc63bbe3721648eb5bd26f10e7e1851b7dc4e4047cc8cc042d46
  8dc
  - 49625ad9fae71ef46bfc59f09cd74d96bd6fe82c24a4f69efb78662addd2a
  320
  - b76d2192812dbdad0579b00ab61a9cec66e1ecdaaac07c36dd5b70bfae3a0
  bb3
blinds:
  - 6efdd3f587b7a0a50e49ababf7cbc908b345f1425e0b8d43b3452eb592b26
  f05
  - a10eed1297b917e6d807866410307f611386858a1bfb528a70c96d14ead9a
  10b
  - 5291910b64461416cac41e11ceaae17db031c5f1fd36c070f2a74b6f66a44
  704
token_request: 00052d406044d05bfbb5643c595765bd6e0cfdc87714d73a43
a0b7e1fe4ef5a9388e86d97ea45908db7f5dad5573a439ac85262f2c7aed0dfea
10f666cc2a7bd79027cef351e6aa090f165739bd3a07d0f456157e8d93db0c7e0
5603bd995936cc98c6321b
token_response: 4060a2740f4d68e9450a975233ceaeaa1d0feadb97ec39346
3ac783c37af8a9b2829e2cd06c01504b39737bd06ac041910e270c18cf6800243
fc1187035c9cd88d45c8d7d3153dd911f6e5724cb0def59739a1674e2ae4ca1ca
f1e5f11e686457140e4850db347edb252aa4b1004f237318f6079413b0693605c
f591b7291d8cff0b659bb5ee237374bc76b5836e5d9535e0c4bb39c73dcaf0597
340c768a6eab002
tokens:
  - 000562dd654dffc63bbe3721648eb5bd26f10e7e1851b7dc4e4047cc8cc04
  2d468dcead0d1e696ccbef94da0dd33e0e265d97a8015532f429d968fa41fb0
  af0cb385ba9dc18997fcf0439475b67cb5a534250d2d25f9c402f5b4f17d9c2
  d37049f2d072877130cee8e7e5d701807193c2768ee9a15726ea564a2bd9f95
  1f2acb90780f177fc8f5a3a8e1248a2854430223634b0aac66f9fb2f609ac5a
  4ee223b2024
  - 000549625ad9fae71ef46bfc59f09cd74d96bd6fe82c24a4f69efb78662ad
  dd2a320ead0d1e696ccbef94da0dd33e0e265d97a8015532f429d968fa41fb0
  af0cb385ba9dc18997fcf0439475b67cb5a534250d2d25f9c402f5b4f17d9c2
```

```
      d37049f2da61b154984bda262b0581883dd386c1c2ea772190cc81d807f239a
      404218f724dadc0cb5527c05ba7cae6d5580c713d5b303853812dd2c0f1ae2c
      a9d8de43e67
      - 0005b76d2192812dbdad0579b00ab61a9cec66e1ecdaaac07c36dd5b70bfa
      e3a0bb3ead0d1e696ccbef94da0dd33e0e265d97a8015532f429d968fa41fb0
      af0cb385ba9dc18997fcf0439475b67cb5a534250d2d25f9c402f5b4f17d9c2
      d37049f2d61df6682b5bf4f9cc8023e6ea6925767f838b0102c06422d160421
      8eb9fcc8f6de083de3f007fa046ded66366e9c7735181fc6c342e03c736f3d7
      ba2c11925a1

   // Test vector 2:
   skS:
   3435c4a17cec27459c6761248b4768b6a580a1ee2cd58ac31fca4af85a171208
   pkS:
   f448c01ff45ee2140d7fa97a4c5944df4aa862408e5134bfc468d40072b9537d
   token_challenge: 0005000e6973737565722e6578616d706c6500000e6f7269
   67696e2e6578616d706c65
   nonces:
      - 97c7bc12d1eeba7c26ee40a120948d31ac622e51347669a908e36ef5fe280
      bc9
      - 5375bf400d7302584be4328f16c385989dfea8d16d9fc18156edaa167043a
      446
      - 43341e4a06021cbce77c21039b6cae3dc8b7194c2f35c991e94157e7fd214
      9f8
   blinds:
      - 41a0baf5b0f33d80be266b014eda0825e7ce10769de0e777faf3e6b673005
      e05
      - 7012a8096a1711f7160bbc11cf6150c8e7f844d955d90d196a2ccdabee3bd
      005
      - be2be22c3b0ddad6edac10fb2201a7b1388d534ca0cf3e03c749c3c65d86a
      90d
   token_request: 00056d40604a4d4d2c54280ab82e7d81277916d12c058f13fc
   2e6ae94d4066dc61087c102f149f790c28f6382f5c8ad67fa6af8e1be1f771ab2
   d2281a09b515c483dba85049e3f9e6761c65f748270e5809b1f992cf1d1834266
   b4e1a3cd389bd78f68124a
   token_response: 4060b6259e46d25a8bf48f25f673c2a0f80c84c6013d2859e
   ec86eb865e26af64f48b48f7c92a124e2051414ac40c5cadadb8a55f0f28bc00d
   6be8373cd22b1b391da6afde766f7e2dc0b2d4d9e7c23fc50a22b5d9028ca633a
   7bdfe4e3bf67d257ada56c9d8723db2220a4f4190c8541d8e8552ad34b30d9a65
   c94347a96a6af00d4b65b5b210471bb4413e184ac5ec98d246f3966132d7bf437
   8b0810ae588a307
   tokens:
      - 000597c7bc12d1eeba7c26ee40a120948d31ac622e51347669a908e36ef5f
      e280bc969b53830c9e88ce2285efc18a8bdc36d2225a41c4afdd0ce1337411f
      9e7ec0ae5560277b39ac96f35076570711615a322cb2f8f3674e64e173873fd
      9f6d6b16deb93ae2e8cf5b447d11bb667e0badb5b191da9639649ab9a4946d1
      e59cf2b2fd2df8de212a34442c1ed4e43108d2fb5f317fb207d902beeb210b8
      f2f66a132eb
```

```
    - 00055375bf400d7302584be4328f16c385989dfea8d16d9fc18156edaa167
    043a44669b53830c9e88ce2285efc18a8bdc36d2225a41c4afdd0ce1337411f
    9e7ec0ae5560277b39ac96f35076570711615a322cb2f8f3674e64e173873fd
    9f6d6b16d5ad6aef9f83b53ee1817cb0b0aac120683fbb3cb2c1e86adde52c5
    33098cc2906bde25974eb9b62132031eea4c8037a187b84a2d406b79e55b8ed
    f7f9b84810b
    - 000543341e4a06021cbce77c21039b6cae3dc8b7194c2f35c991e94157e7f
    d2149f869b53830c9e88ce2285efc18a8bdc36d2225a41c4afdd0ce1337411f
    9e7ec0ae5560277b39ac96f35076570711615a322cb2f8f3674e64e173873fd
    9f6d6b16de487d2826e4e90e2e2fa24df0fdb89ca90ba900b78fb126553d77a
    4bb11ac5fbd909511a35c53ca45841ceb32bfcfe27a17fbdff9b942c0aa8fed
    22b88d79d28

  // Test vector 3:
  skS:
  d53e857d8c589ee11a175a4d880e498d0433e439a72c6ac7f8222873dfd89e03
  pkS:
  7255025c90d76238ced53cc4473787ea167a7017ae0c1d63e864d599ae5db452
  token_challenge: 0005000e6973737565722e6578616d706c65000017666f6f
  2e6578616d706c652c6261722e6578616d706c65
  nonces:
    - 2607568322aa05f59b5a01ac87c3b55ad11e9bbbe60102af0c5c17f6b99be
    c02
    - 9a934eb5a70436aed6afdcf2460242912ddeeea160b39839bc233de6a3246
    b2f
    - 7555220de2ac527a9c2fa2e10ad239543e2e846245e6a76a7283d1996a878
    251
  blinds:
    - 8504535ffbcad52af25c847250d33a4ba3eec29e79b282956d5b68348eee0
    802
    - d85fac3d7203ca80792f8f9299420aa0f93564297fc1c6f2d8713f5181747
    60e
    - f3bdcf1cb48cb0c10018d25bbe4138580cd90c9a0b78e3684b219e0329d0d
    609
  token_request: 00055c406046c5f2c875f41a6e75e579186b9f6b0c60fcc156
  1cb31227a0212a6fb122a138724033cc8d9f03aab1ce5df56fd241dbdbfb4c5ea
  6cedc82d8e95da3e3da804e000ad869035bfb0d673522d0bd94b8ee75a5b79f8e
  77d66107804aaf73fb863b
  token_response: 406070c40700200f461cad7d144d352cf99aeef2958f75442
  3bf04e92eeec2a6c11b74ce8cc8fb24780d1d4c67bd74e57ada3901a2dddfc3ef
  088ebbdd45daa54b3ff0563e59dc3f4f13fc574058c907468714113e6bc2dc421
  c05432d757d518e553df0b206dc7268c08ca9bc03f67bd1ed92c7b3ee62bd404d
  9c17dd69066deb0477506b8a404ad27474f71142db91e549dc0d76c44e099e3f9
  6b71bf292e72a01
  tokens:
    - 00052607568322aa05f59b5a01ac87c3b55ad11e9bbbe60102af0c5c17f6b
    99bec028a73b15843d93251b73e17d484d3e5467e6db28a74a042d83a311005
    dfdb9c61af60e2f82acdafaa9d3c6b8debb3b1b4385b3357f0cf60441f97901
```

```
      91fb9865c82d2beaae48321c6e376f3190dbf2389b2d717481ec73734dd246f
      397a217f0894eff9ef4ad3f110bf265285148a657b20c00457cd03edc1f3d6e
      6268862e2de
      - 00059a934eb5a70436aed6afdcf2460242912ddeeea160b39839bc233de6a
      3246b2f8a73b15843d93251b73e17d484d3e5467e6db28a74a042d83a311005
      dfdb9c61af60e2f82acdafaa9d3c6b8debb3b1b4385b3357f0cf60441f97901
      91fb9865ca959e4e6015c1c5b877ec82aaf5d1bbf4fa4b58b684b2c1b590264
      99c998768cb87b17f32fcc8dbf04509e37d72810fea6e4330341deecb2d6fa4
      7d974208947
      - 00057555220de2ac527a9c2fa2e10ad239543e2e846245e6a76a7283d1996
      a8782518a73b15843d93251b73e17d484d3e5467e6db28a74a042d83a311005
      dfdb9c61af60e2f82acdafaa9d3c6b8debb3b1b4385b3357f0cf60441f97901
      91fb9865c7258d95e545f122c90e331633177409277dd59fd78e4b51b88165f
      fa778b1ad019af5ee8dff21fe58fa0e31fd4a2ab0512b4ea9c487acccdca544
      fa33294fbf0

   // Test vector 4:
   skS:
   7f52844968e3b9ebeb82f8930bc02af1ae35a91e9d699949a629f351e7b3c00d
   pkS:
   182d797eaec74157c6911f105fc7d99fb08d567e3da7bfefd50340594c603345
   token_challenge: 0005000e6973737565722e6578616d706c65000000
   nonces:
      - f8534e3448df368adde4bb0609b58799425372e25359922d9382491d35525
      1bd
      - 4d8c92091880c44bc24d5396ecaa68140f65ed3498a72d940bb651b3a952b
      bfc
      - e1f48c0ca3847ede3309e4b13cbb9edbbd65e3bfec548ba80b3193f96336f
      d84
   blinds:
      - 903382c558a850f936d8a74e4ad54ea540b451240b8b75ae65852b78e4545
      e03
      - 477e6b85f1380a627627e37d07466023f73bbe60dd6de2d47c9c6f8805a73
      509
      - dffd7898231d883e1b2367f97077d868c2d5dc0d454ac2aa74ce077133cf2
      b06
   token_request: 0005dc406062beaa14db5c4d720329060e48228969458db99f
   f6c9a67a8fa2652f4da1b751daeb2ca361e24b610585e52c7a98ddc10c381d988
   aa93ddb490024690884471e8a8d702f17f62b60ea43b0299586d4f01d800c6ace
   c318c921b27c3457358750
   token_response: 406000e8ca4ba785a65ee67460c8ca95e31a4e29b86cdda7d
   3bdb59ecc471dd08501dc73c0f433876b3bddb6a251f06a056b928e0ce9202d14
   a34c7454b1bae7a164e6191c065b9387302241f89a636f742ea754b17adba4979
   7b0ec60c0690bde4b5cbc1307ff1766a3997897939c5bf404ff7396462f408497
   d78f4a4f2b73610d0a827e4f85a1995b9a7bab72cd982ae8c52d7a994584a177a
   03d4e1de4118608
   tokens:
      - 0005f8534e3448df368adde4bb0609b58799425372e25359922d9382491d3
```

```
      55251bdb2174d8c51b010f2f8d73a85a8595138f02c4082a27c5348a4767945
      6d9e350fba3d0d2cdfdcfa32ba7e5a520cfeaf05057cacfc374fd400493067c
      1e85e79dc070ae23afc8d8a81e448a4abf0a8e4f0cf2c285d9c7d6707f0b817
      3fdd9a007159c5351e191937d22aa58dba713f541d2ad54e9b25af63b68a0e1
      060b0a9611f
      - 00054d8c92091880c44bc24d5396ecaa68140f65ed3498a72d940bb651b3a
      952bbfcb2174d8c51b010f2f8d73a85a8595138f02c4082a27c5348a4767945
      6d9e350fba3d0d2cdfdcfa32ba7e5a520cfeaf05057cacfc374fd400493067c
      1e85e79dc0cd9ef54f8d9a456634af013b7da99e4c52cec576c283ee64a92cb
      b9a5289ce76d492c423f1213b6b3bc7d15c0ecc15a3f663f1b99b59b7667b3a
      8a4d1d7794d
      - 0005e1f48c0ca3847ede3309e4b13cbb9edbbd65e3bfec548ba80b3193f96
      336fd84b2174d8c51b010f2f8d73a85a8595138f02c4082a27c5348a4767945
      6d9e350fba3d0d2cdfdcfa32ba7e5a520cfeaf05057cacfc374fd400493067c
      1e85e79dc9a05c3e96f3abd4e4ea700eb67c95816f76ea423dada2d699a7f92
      328cd9be5d83e8f77974e930d4eee806599efa0d6f3c37749337d1223901a8b
      60e1bbf991f

   // Test vector 5:
   skS:
   5f6b12eaa6bc82618be24bacad324ddf88bb2ed80ea05e1c09c78ebb33ca2f04
   pkS:
   0af469e5ebe48eaf5ecc30d2a33e715f15aa18f65c72ba7f729331b1f4fb847e
   token_challenge: 0005000e6973737565722e6578616d706c65208278149d30
   94c9138347d7a2bcbf1188a262a10b1a5696c41549eabed84c129d0000
   nonces:
     - 68286e9d5a447f04dadb444fe70c01e89f14305d444a462e5a38b154b6102
     961
     - 921f1cd630b4c1c975a077caee796afcd2bc91dac0891e131ae0744cee4a7
     595
     - 58f3e3da23295d741fc9209b2e01f486ffc5bb4cd9e01b52e2ec22d881062
     eb5
   blinds:
     - c494912581ce9ef0e5cb5a45be546c7df5bafa223b9f84188a5bf0bad72b3
     607
     - d91de980016f7dfa0b26f303f46bdabd70d23c57720a8236117aa04ec5cbf
     e0a
     - 0fb91d23a8bd9cc34d154be0fb25b522f8d90da3aacee22abc0823586c6cd
     50c
   token_request: 00058140603a1d1b2e8a9d73b19dbaad85e8c53611dba68236
   273a876b85e36310f68bc71b1ed45cf7ce982516f6fd79047fd2fa974a04661c9
   dc015ec44c48f3a8f421104ec506f251d8d3d0738397f4751078ba1bbbf34d9a6
   06962900517108e9935759
   token_response: 4060085b0ebcdc26bc0c86908f5faa30b009188e199972cb3
   fadbe144bb5cda0bb5a209313fcce1bb4727fe4829e220470d6edce2f119d206b
   0fc94208e3dfbfb612d44fb3af8afced1d6efbf7a81f0087e8e1c9384f3a70153
   164445f60ab134a5dd3e48dfe1d0ce4a2ccac03c74d5ba6c6c854241019693bd1
   e0ccb94458a4600a07ea62971534362965c8ff6cc4c956b849547f656f7d5ce3f
```

```
   cc0fcd626b34809
   tokens:
     - 000568286e9d5a447f04dadb444fe70c01e89f14305d444a462e5a38b154b
     610296176ee4d34d93248d8759177310d19ff8690ccc42f86793cdac0698466
     c3c70da43a9b33fc1983a678ae21c1d544a7340ba7a82a180a9b34ae30db22b
     9ef18a981589c0784cba583bb7c1d2ee684982f706150e8c1901f6dde04abee
     94bbffff08d43131a2a596bca267038ad065a091977014e26af3bef97023122
     bcee8394f71
     - 0005921f1cd630b4c1c975a077caee796afcd2bc91dac0891e131ae0744ce
     e4a759576ee4d34d93248d8759177310d19ff8690ccc42f86793cdac0698466
     c3c70da43a9b33fc1983a678ae21c1d544a7340ba7a82a180a9b34ae30db22b
     9ef18a981fe4d8af90b00fa6324d754e9d318344b86a491d49d03da598c440e
     9bd84ca5484c98f4b9c8a431e3e54dc36bea34a0b15fc9b527337e49a33ebf6
     48b133101c7
     - 000558f3e3da23295d741fc9209b2e01f486ffc5bb4cd9e01b52e2ec22d88
     1062eb576ee4d34d93248d8759177310d19ff8690ccc42f86793cdac0698466
     c3c70da43a9b33fc1983a678ae21c1d544a7340ba7a82a180a9b34ae30db22b
     9ef18a98133451aefec7d96d9fa9015f8c4f36145f0d46e6d0b1848e54120a7
     c531fdab5fdb6687c0b9cb797bbe08ff19779fd420d366b54525dec516d60ba
     d56ad1b7968

   // Test vector 6:
   skS:
   67c58e0233699e8786ed481ed3a0151bfa62fca99473a682ea3bf1f3b9638e0c
   pkS:
   e0c927df150241463b91bffdc3ec1a502bbca530387ff122956dac5aaebb8e39
   token_challenge: 0005000b497373756572204e616d652045d8b12d8bdd6dcf
   4a55ab3d9d44536452e62ca9e184499797967b341598d5b30005612c622c63
   nonces:
     - 1759d45e97a6e2e6b8d748873375d17cce526d4915e502409df622676125a
     e7e
     - 8d9cb210755838c466b1cd1ce85dcc490089107b7edc0b78e7b322c2e6b07
     fec
     - dc72b81f442b881b652e8735f7998dff752a9308155cb0d249a4f3f2a5220
     4e7
     - 3a4c77ed3e8060b900c32c2fb096427cebc034f376d72d41a61b3ef834470
     076
     - ccd62be47ef590ff3c5368c79c9abf860793da279d8eaf2b912cfaab84660
     1e5
   blinds:
     - 57530d3642417cb45468eba4d57c7bd20bd0d5eb8945862b2ee946e8ee6fa
     20e
     - 5529fd3d3953a9da6e539356ea95a3107c8381827c6809b9697a7a9f903d5
     c0d
     - bb6eacb12745b1cde1c7c54c9b1b733a126c5d5fa12ac88a81fd785df655c
     701
     - 99b7bd5417c246d02530415713cec68bdf595b8b3854e3c6774e3c85e1f3d
     80d
```

```
    - 513d0a4e63048b2360ac70006244bc0976d926ba9423fd08d1dd6fdfe7793
      f01
  token_request: 00056a40a03c91a8f09540be56f4324bd7b42ce3a951e29eca
  1db6529bb0372950913b7c6726c58da089b13a619840087484ee5f35eb4e04b4d
  fe723013024f9d4522b205930af1bf45d6806a946f19c7845b7ecc37e0ecbb077
  fbfb9a35b71edf0b80431232388fb40822f9ba56947baf200507ee0f95bd4a54a
  a0322c5b00d95828c3e5b247daa33bbdf0905f0a6244fbdc3403352a22bdc42d9
  97751c6b820a77c9b917
  token_response: 40a034269e1def8ec92e36be666f4f20d7947b3e0ff52ca46
  b238ec5f7b885c3dc1336a48658f72e52e15b57c29c36e00a82150f8f9970d0a4
  665ed51be99d466273fea90054904852cbf4c9885a2930a6d3c0a98207fe5ea73
  65a17a92b0294c46f6c774e99b4e7892b60f2f3203e6557d9bbc77006f89ad980
  3a14387b78a12d76147dd6156983f14b1d1fa7dc07572c07bf6292258ca415830
  560a473baba3e48ce0281645b5e56cbfe83a47cc9be3bf0ace9d133434411cc25
  c9bd2c93b60108def27bb7d5e19015e01f94b9a484949649c7264d02432839469
  6ea36ee192d03
  tokens:
    - 00051759d45e97a6e2e6b8d748873375d17cce526d4915e502409df622676
    125ae7e373d5befaf320c32753b4d65e945224101a36faf414d1988c96cfd5c
    48dc378785be0d8b69dec0751ea2fb6d6e26ba6cbaec6c2e01c5d38a1159d99
    574584b6a40138d77a91f365366880d40b12e776a45b3749a74489486a48617
    7c364980bfe9e52a3b16c521e54c1b75a0f73227e78579c66108dd1068f543c
    b293f22e7ed
    - 00058d9cb210755838c466b1cd1ce85dcc490089107b7edc0b78e7b322c2e
    6b07fec373d5befaf320c32753b4d65e945224101a36faf414d1988c96cfd5c
    48dc378785be0d8b69dec0751ea2fb6d6e26ba6cbaec6c2e01c5d38a1159d99
    574584b6a56279c71e27fa1f4c47db14d1b648b1ce638398c9691e2da380b7b
    d14f3041932760ccb6edc815bc77f1946d258da46096df4f8cfa7a4249b2c90
    9b875bbbaf7
    - 0005dc72b81f442b881b652e8735f7998dff752a9308155cb0d249a4f3f2a
    52204e7373d5befaf320c32753b4d65e945224101a36faf414d1988c96cfd5c
    48dc378785be0d8b69dec0751ea2fb6d6e26ba6cbaec6c2e01c5d38a1159d99
    574584b6ab151994e57bb02bb2212b960a4cfc73ecf3b3e3b1161e8a9730cb9
    2b9be95641287ae256b48033014d23e828afd97ac05dff271fb4a6d19113b13
    9c8deac2059
    - 00053a4c77ed3e8060b900c32c2fb096427cebc034f376d72d41a61b3ef83
    4470076373d5befaf320c32753b4d65e945224101a36faf414d1988c96cfd5c
    48dc378785be0d8b69dec0751ea2fb6d6e26ba6cbaec6c2e01c5d38a1159d99
    574584b6a0436b98b5076388e09beb78ad871e7b69b3a647e1f7fc9a7bea268
    e3d324d95a73c96e976ef4904b17ea6217679e0a30fa4e66f4e18135c4b46c1
    f28d23c60a7
    - 0005ccd62be47ef590ff3c5368c79c9abf860793da279d8eaf2b912cfaab8
    46601e5373d5befaf320c32753b4d65e945224101a36faf414d1988c96cfd5c
    48dc378785be0d8b69dec0751ea2fb6d6e26ba6cbaec6c2e01c5d38a1159d99
    574584b6a3bde0f53c3e3786c6decab448cfe28b50141f00086c01d739bd516
    7af4124ebc3848eb39574941814465c3f66423f567d4d6592ddfeff44b65cc3
    2eefb7ed271
```

```
// Test vector 7:
skS:
ecdc82de96472dc1c50fac8326b0107da2963ba7809315656df42c6287e3c50a
pkS:
843a063ff826c65b8cf6837650cf8fe6fa846170b63d324428de46c4a3a72045
token_challenge: 0005000b497373756572204e616d65000005612c622c63
nonces:
  - c87deb2027bb12c630acd37dd86f92c5b294a615bd497cefed043cb4181cb
  9ff
  - ddda05631e907f9ca69460f70b824c4a74f350797597384c9f83d0167dacf
  d7f
  - 9783a7a64bbec7f6857cdcdec127074c8083c6d90ea8cfb40281add9ce9f8
  206
  - 7d559e4f5ee76bbc5d6db924c41155bec3d2711b78d829b661f2f2c2b4581
  871
  - c81eff11d41df37ae9deb5903fe285a179db49e06724a4a98390debdfdf01
  735
blinds:
  - 7e9c274897a2eb4d3c81f92adf8d57a65f31a2d62ae2cd6a082067a858e69
  c09
  - 210b60d6d086a359efb0c8461b721c7ecece79fb1898bc1701054f963cdf2
  60e
  - 004913190243f32ed091a50c6ae401b7d642c8013a2adf076d17306351c60
  60b
  - 50dfd8599cc2b57167cb92652cc4293383aeb3a7f79d1505b9ad3e9745da9
  c0a
  - e2f26157371a2a2be676989d010b0d41280bccffc03e540b67b1fdb05c23e
  500
token_request: 00057c40a0127758ec6139139b85bc167ec0b3281648a7cae9
f4b81b4cb3e29343d213265c44dd09ee22354e72599819cc45a297740b15e4c19
9a39519dbe64ea21e564a00c6d94a82c45bcf99f565b6fbd5dc9434382a842a74
fe9020b481551856c889083acc90c791e059126a503471e67e38187a7096cbed3
f734f57a5173c0e5c4967f842d6b172b5c6da1e3bc60aab65808b710df4311ee9
fbde33defcdf97a2617f
token_response: 40a05684e8b68dab1db207daa489c18cb88f7e6447b5e6939
eb82b9a8c8fe460cf6484d65dd432d0aa502f3cc2189e3fefd7be5d65cfde4e5c
fc240415a2d6277e2c9a56d40ffe2e9b94bd213d904fb933c8df00f9e299f9c64
62cac4f6b8a9eb620ea717614dd6bcf6875474bcf7cbd5e63ed5cd8d2501b296a
4839b6cf68c6957b82582103fdd6fc8881172672c38452d9643957fbd0233681a
7ae01eff600aa5eda561521a61fcffcc385e065a1a99edba16cae4cffd9eb31ab
1c0b3cec072e0c1d6f3bb1327f93fc56184773925f3bd3a5798f3543adcd14d16
f27217e796a05
tokens:
  - 0005c87deb2027bb12c630acd37dd86f92c5b294a615bd497cefed043cb41
  81cb9ff05bebf3881b04fbb652613bd335710fce992e473ae4c5d860066d5f1
  5535bcd13e76fcc60625aa80197b8fcb32a4ab21c2cec08fafddf2627f25c47
  b6974c87c89b95ba3decf698ff3dbf619cc57ccd79e906e9de1d2635b52b46a
  9397c7e7b4495c00edbfa88c03a462985bf7a273708f1a7404206b1fff15a10
```

```
    ebe894116ca
    - 0005ddda05631e907f9ca69460f70b824c4a74f350797597384c9f83d0167
    dacfd7f05bebf3881b04fbb652613bd335710fce992e473ae4c5d860066d5f1
    5535bcd13e76fcc60625aa80197b8fcb32a4ab21c2cec08fafddf2627f25c47
    b6974c87c2bcf638aa8b6935f6a7774e017af3572f4a14f7fd7af1413ce9c48
    81daec3a62448029009461cc6d39a7af0bdbba67fa4a289a5c6b64c12e63671
    205e1cd5114
    - 00059783a7a64bbec7f6857cdcdec127074c8083c6d90ea8cfb40281add9c
    e9f820605bebf3881b04fbb652613bd335710fce992e473ae4c5d860066d5f1
    5535bcd13e76fcc60625aa80197b8fcb32a4ab21c2cec08fafddf2627f25c47
    b6974c87c8c96a6126e31bc967715d6c9baec1ce9666c309ce1cb61317211f7
    6932b278746d732bf30b86b197266d01279b22d5c78045a507d7b6eee4d1947
    94996c32cda
    - 00057d559e4f5ee76bbc5d6db924c41155bec3d2711b78d829b661f2f2c2b
    458187105bebf3881b04fbb652613bd335710fce992e473ae4c5d860066d5f1
    5535bcd13e76fcc60625aa80197b8fcb32a4ab21c2cec08fafddf2627f25c47
    b6974c87c8501f8911b3cbcd823543ef9611f4838761df61b35ab9bac272980
    49cd5e4bacc182de6f192453993f63f02531dc28ce51c7e2ffe330e63880c54
    e7ac797e602
    - 0005c81eff11d41df37ae9deb5903fe285a179db49e06724a4a98390debdf
    df0173505bebf3881b04fbb652613bd335710fce992e473ae4c5d860066d5f1
    5535bcd13e76fcc60625aa80197b8fcb32a4ab21c2cec08fafddf2627f25c47
    b6974c87cf1c8a34db360b9e03b63991677d003ca9b001496edb9dfc8e0a779
    d3169334988434ad729af8bf771c1d6b239674c3ace1014a15fe392185e504e
    20ac2f02fb5

  // Test vector 8:
  skS:
  d41d8dfc86a0e0ac23be4b8d07c296825e72d349d25adc52955c7a4096d5ea0a
  pkS:
  aa2afd7eb2dd901fc673f365ed09e41a99c52eafd9035cc49ad7007cff40e022
  token_challenge: 0005000b497373756572204e616d6520a2e454dd86916617
  200734a794b39551148b99b83ccc30ff8a31c65c9dcc30120005612c622c63
  nonces:
    - 5c71ce1399c248c7fdc1784e6b6f4321d26f44b43b9f51391e9851a738ce8
    c99
    - 97ff5e8a2c4e068de508d7854fe12ded84e7be315910e34e0b61e5eb2b5f8
    806
    - 69dd91196091b4a6ff53b94bed94de141d0514c1071392fb31e43122adfe9
    82a
    - 08a53e1026c5d6a7ab564361268849460b497607884bf40a8782b5b8eacc8
    166
    - bef306b3b764e961f87c15ce250219cfc2ddd673485afb50777459e56f9c8
    c23
  blinds:
    - 9e59aefb5780839c60c8cbaa453f1b2928018efbc0e31045e89559fdb1034
    108
    - c6afbe1f5e10ea7e59b0e4eb819fa3ef323bbb43f204a59df4cefb2cce883
```

```
    f09
    - 2c08703c5d12f2bfa02605438f2b56e6597a8ed4f1098256b4d8e6cc2021e
    203
    - 0a474bb7b278f33e04bb80934dda994f6313033c352abd2577e43abb5ed9a
    d04
    - 592345198011d91d96be8c374cbfb138bba1360699b6abf60f43622f0e70f
    b0c
  token_request: 0005d740a0ac3b0159be73652492a2d257c505ba04a56f86f6
  9fb0824fdfc6146d4ae08f2348d02da2cb4b3b9397972714d718353185031fe7b
  a55cf2b135b38814921592fa2f77a41ea94c0a89c807bcf5d57ba853a9a09a8aa
  64a237a274bb1ae4fa307a7274cbf8d9714184911d48b4f848cc16ee463557d7b
  9c7469309d8a9f825c5316e77d093b9c48f20ab65fbe1b097d20a4d76a954f687
  a2ea1575feb98690be48
  token_response: 40a0a20a2228d39c8b152d7c880fe88d0e097b13d75981d2f
  0332890a81fa089cf1c5418aceb7d9cd6db3bb5d74f7260d3c8d2d5bb4d2b0213
  9d75ab41563e986a47382fdf4f6cf4d185b6cc90fc21a404b3a507336ef01ba9b
  ce56de1272de3100ece040ade1f57c3ef5d71a4fb69ba22eb54f4854f13c894b5
  52ef5852d590e946365a89f3b01c472d2932e4ea42be4c6c55e42c5dd5b1666ec
  7af0e932ca6aa218c54b43d0014b9fad7e9b5304bc56c57e10516222e9d23e77a
  79a2fb452dfa0aeec5d1806242981edc3aa3a03e054774b756033e5e1053b803d
  3c5a6bbb1460a
  tokens:
    - 00055c71ce1399c248c7fdc1784e6b6f4321d26f44b43b9f51391e9851a73
    8ce8c99804c271aba5a1735acbc0ba3312c127c9435a3ca073f20e7a3c04b0b
    ac5e8a52a69e0f18a2187cdd2f124a837dd4c06a33393467c7c010ed0757631
    5559ea0d75a1e542038ee670d0d3a740f0a811215d765487470eb91d34deb81
    e033d42948f5fbe4c1062657decf49bfe29b2c16c25e80b699eee20308d45df
    abb36232c36
    - 000597ff5e8a2c4e068de508d7854fe12ded84e7be315910e34e0b61e5eb2
    b5f8806804c271aba5a1735acbc0ba3312c127c9435a3ca073f20e7a3c04b0b
    ac5e8a52a69e0f18a2187cdd2f124a837dd4c06a33393467c7c010ed0757631
    5559ea0d7d4e80104022b0ffecbcf56655791ab8f8f9b14be57cf1a150fd866
    b770eab79f8806757f29ca44e6d9a4dd68d583ada5704082c2bb9036be340b4
    37ddd7c9012
    - 000569dd91196091b4a6ff53b94bed94de141d0514c1071392fb31e43122a
    dfe982a804c271aba5a1735acbc0ba3312c127c9435a3ca073f20e7a3c04b0b
    ac5e8a52a69e0f18a2187cdd2f124a837dd4c06a33393467c7c010ed0757631
    5559ea0d72091c81218a09e8451aefbb33963f72fbf8120f4a353e6e8ff4707
    322f987a5c6f1ea3f29a843755ddc1144f83675589ce444ac6662e5a14c6eb0
    42b36ea8031
    - 000508a53e1026c5d6a7ab564361268849460b497607884bf40a8782b5b8e
    acc8166804c271aba5a1735acbc0ba3312c127c9435a3ca073f20e7a3c04b0b
    ac5e8a52a69e0f18a2187cdd2f124a837dd4c06a33393467c7c010ed0757631
    5559ea0d77c82958d196cc8195a648adf3f8318684877df551a0029e5aed482
    cf057ef12f374e33e69e82da060415d131a160493f7fc5983df5e0d91eb241e
    11e4549e9fc
    - 0005bef306b3b764e961f87c15ce250219cfc2ddd673485afb50777459e56
    f9c8c23804c271aba5a1735acbc0ba3312c127c9435a3ca073f20e7a3c04b0b
```

```
    ac5e8a52a69e0f18a2187cdd2f124a837dd4c06a33393467c7c010ed0757631
    5559ea0d7ca2d5d11b8536e2ad6c2a52125be66e2e9e6af7ccb0b0ec6ec814b
    25e656cf62d7420d6f1362ae8804db20c125f2c65ce8c89295c55be3b30be7f
    26381374796

  // Test vector 9:
  skS:
  555af92535f6fb5995e68081dfc355687f2634590a78f3c86d3f43a53f32690c
  pkS:
  ee2e64c24d283fd49536bc3ffe71d8959292f804a57de7ae96501cccd87bcf4c
  token_challenge: 0005000b497373756572204e616d652047ff2caf91b609df
  6a34b6570d2c78853dae84f281216e614b4610d290c902f30005612c622c63
  nonces:
    - a57ae0fc3c01801e041fb461290d3f5ea868b46769b3d81a280fd92ddd11d
    838
    - b5440ba986b14357200adadb6f0c451bdb994eb46f21e72606fc53e364413
    f1d
    - e951bc70783af68f70f0397c3f2694ec20a0552b352dbdff4682f7f7f5fd5
    cc2
    - d737b094a9a33d91efc703aecdfecfb4092679f29ec79e1d0d8eb876113f5
    827
    - ae0634d5f777efb338e6c18df0d4f0b915660e5327a600c1ebd118b16e06b
    fbd
  blinds:
    - d068c9dfa0384a414e3f0ae809be8393e03563137360675c51d2b5222f38e
    10f
    - e129758dd65801b25343004323597f92002f2439f23ca73c29e606e024218
    e0d
    - 07403e8dc6794247d96bb420638ac13f805101172b2dd32b75b8034f29e3d
    a06
    - 3e8b503edae054c279d12fcef1a60af4e43411058eec0f2bb5189655bb9fd
    709
    - f84234cab822e97319ff0ea7017602352bbc27c32bc4b6c487a4f8cd30ef1
    802
  token_request: 0005c340a004a20e603570f1e2853e036bc1b68cc11bd96a7b
  e6025ff25f391273439e491586e34901269fc21dc59342dc99f0677d776e6ea4e
  a5e6205c885c54b0b09dd1a5ef30afe4cee5b390bbe8b5d4a0fea638c4eb9996f
  dd385d5318524662865533a4ea1e1bc4608685d1ad03ff40e6928acdde7d0e2b4
  5a563e3ec7b5ce1e25e147a64d26cb5061b83d0243b44805e47aab8f860e39f67
  67ab82cd5b90c7a5b843
  token_response: 40a0229fd94f20d892c68d3ef41cce82e8a4bbe055af8200f
  ccb1ea798ed5195045f924fb818fb8e0a6ea87f871d45c6f640a01f9454c72a69
  662189b6a10875d63572f6e51c79513336fc0d0a78082c7d12c929a0349ce1afb
  be446c73f08016e456e6921da097ebb8156f19f9e075b6b58f7e5021ef9c98161
  30929c7ce6adce09a0c782e0115c7ba7a2ccc17d1166dba0ba16f957dc2391a98
  bff065528269d5b82efc1d3799dc1f2d0ba2ce7a86c319ba4be0da261e517e532
  80276ac106ed025d890ad3e15a79e0a5004309ce00e9cd172392bf45042e5ed7c
  865592d17780a
```

```
   tokens:
     - 0005a57ae0fc3c01801e041fb461290d3f5ea868b46769b3d81a280fd92dd
     d11d838f8a5f2a01a1ac035515fbc59f5501039207a0406c3ffeef924e81f93
     cb41381f1daf713ffbeaf2f3a1549318cbcc6cdf9812c150a7c63bc0a07f138
     ea95392c38e79b42b2206cc1c5b8913eedeaeb35563d567ef46f7a0f84a5434
     d840d80e579db1109548e30f130f048579b5a5d2e2c4da489902978fb55da92
     ff6d1550dfe
     - 0005b5440ba986b14357200adadb6f0c451bdb994eb46f21e72606fc53e36
     4413f1df8a5f2a01a1ac035515fbc59f5501039207a0406c3ffeef924e81f93
     cb41381f1daf713ffbeaf2f3a1549318cbcc6cdf9812c150a7c63bc0a07f138
     ea95392c3883ee75d5b5605a25d7b10208a85ec8e6051167ca2435aeb80f2aa
     73dfcceef9dd52075f74c95741bf1cc4a2071bcaf4ea8f34aa3fd0d8a7d19ed
     7d58cbb3068
     - 0005e951bc70783af68f70f0397c3f2694ec20a0552b352dbdff4682f7f7f
     5fd5cc2f8a5f2a01a1ac035515fbc59f5501039207a0406c3ffeef924e81f93
     cb41381f1daf713ffbeaf2f3a1549318cbcc6cdf9812c150a7c63bc0a07f138
     ea95392c36e7b064de9ee05b86a4b44bc9cedd88ad9562ebacc4ad372947828
     635495b419f9ceb094ff1247d19e4b603fd5ca58b8b343aef1b4cfd38508c3a
     2fbd4505471
     - 0005d737b094a9a33d91efc703aecdfecfb4092679f29ec79e1d0d8eb8761
     13f5827f8a5f2a01a1ac035515fbc59f5501039207a0406c3ffeef924e81f93
     cb41381f1daf713ffbeaf2f3a1549318cbcc6cdf9812c150a7c63bc0a07f138
     ea95392c368d8dc61cb6266df80708591c8fde0e991873640e59547f372d620
     2bd67760e304a1163ac5181288fdc38718d3a9b10c6e42c7c1fa032be8bf68f
     3beea2737b2
     - 0005ae0634d5f777efb338e6c18df0d4f0b915660e5327a600c1ebd118b16
     e06bfbdf8a5f2a01a1ac035515fbc59f5501039207a0406c3ffeef924e81f93
     cb41381f1daf713ffbeaf2f3a1549318cbcc6cdf9812c150a7c63bc0a07f138
     ea95392c317ba664a3e2ed7960691c1ad8b00b5f27e9f43fd59a5a3b5d848c7
     d22732b731007c23207c9b0f27eae535a22c2e5ada78132f103bf459e6d15fa
     522ee7e9a0e

   // Test vector 10:
   skS:
   c8b2a8db34d93d701d2032c82762637e0f06438a38290b31e086df6736ec1a0e
   pkS:
   d40d0da35ae466cd1f3453dc241a049e5562768b7cdd8dbaf33f4225a5bd2f1a
   token_challenge: 0005000b497373756572204e616d65000005612c622c63
   nonces:
     - 826b36a503e94993f1e61f5df51e514ddf5e761e33aed1df52c3516093b5c
     e14
     - 7b9bd7137ca524f027d22ecfe3f34d8962972a9db5a270ed319cebe823eed
     4c6
     - 7270ebf05813dfaebd76f29d4ee2402999a9acaf082ce462479fabbf2a704
     93f
     - 08ac07ee5eee937f0f1a8965e8b0a18eb51466dacd1861bc6e6727c0e140b
     32f
     - 059bb7481ed568c5abcabb533404e464b381a4e4874c1e7bcb1058183f301
```

```
    8b9
  blinds:
    - e52eae97d5adb54e5342802a58df8e684a92ee0b04ba0aea27de70bb9c93b
    c06
    - c30ea35e9d8b5f944f827b624ca2751718de2f1b2a9462e670c743ff095da
    e00
    - 7e7be57b39d9cb937929999cafd8584855d65973ff2e6fa6cfdb2673a95a3
    702
    - 826cdb7f7ee684c14fff206617abfb33ab3797c30575c8ac4236a3e31076b
    f06
    - e4489ba8e7015def8ae292405e9d82aa50749fc86a379df1bb594b839ff24
    b02
  token_request: 0005e540a0ead483adbe1686ec443cfdf0adc6b69e150dd0a0
  59e3b326d5bc9f0ccfe71525dca436c5e0cfdf379dbfa8b735b1660e64c543831
  cb18cd7e3618e3d3aa8a25e8ab9bd2c3b9d073f060b7444b9832c91208af56cca
  f6d6178e7fef2634da3f4980fa8e32fef683a6f91a791306326283f93c2ce3fa3
  0b34457d4d7d9f315f45a6c434cb20291fe064c2b11654a4c3d688b9c5d0a555e
  99ab7d138dfcb3b0914d
  token_response: 40a0fc8b20caffc2cb13aee22932de8704a6c33b1c8923673
  ebd4588f573962dfa7c6c7a47c86f67c2140d4a1de69436ee7f9e44f535ed6e14
  56602a4a065fccf26e82f64498bb9ebbd881aa56815f06606dd189600547a7208
  2059980e5cd0b4c52426a7b70635203b401ce462ab4d8417569fb71e1459c3f75
  5dc3ab83c13c1d56f4948cc85f3e2e96a110cb0cf03a53e552be77b0c27929bcd
  91d535b1419b2586a66a3be0d0dc89752ec343e4798d1666f67e9a813c844b5a4
  9fabcb86fdd70b8a034120ddc2e3b5e8a9d9637898229d3fac61cbefe2b3c02f2
  00d98a318800f
  tokens:
    - 0005826b36a503e94993f1e61f5df51e514ddf5e761e33aed1df52c351609
    3b5ce1405bebf3881b04fbb652613bd335710fce992e473ae4c5d860066d5f1
    5535bcd1f1c2acd113354cf4232d21f040e81e072d5ffaa444cc624c262eb96
    ded70ebe505a11082b20b061fa8cc1b83e3abbe3cdbe03d98de39bb09c9fcfb
    8c85c99edbaf1aced4fb7ecabd0391bef3ec135e35591a627e07d0c34d4668c
    76322d186c3
    - 00057b9bd7137ca524f027d22ecfe3f34d8962972a9db5a270ed319cebe82
    3eed4c605bebf3881b04fbb652613bd335710fce992e473ae4c5d860066d5f1
    5535bcd1f1c2acd113354cf4232d21f040e81e072d5ffaa444cc624c262eb96
    ded70ebe501ef6b44db79b406dd1fc90e5313f93cdc37cbe1616fcfee47919d
    dbb18e79b1c5b59c73b117cca3266bd5cd062865c13f2d474b241dfd6b23321
    85d205a3327
    - 00057270ebf05813dfaebd76f29d4ee2402999a9acaf082ce462479fabbf2
    a70493f05bebf3881b04fbb652613bd335710fce992e473ae4c5d860066d5f1
    5535bcd1f1c2acd113354cf4232d21f040e81e072d5ffaa444cc624c262eb96
    ded70ebe5fcd83a3c259a5cfd9ab76ef64eca274475d0c74860ea549fa21257
    eaed4a22d467f19c7a90dd7840c2d377735f3b8acaafd35bdb2b2bf39cf030e
    4c412c32f29
    - 000508ac07ee5eee937f0f1a8965e8b0a18eb51466dacd1861bc6e6727c0e
    140b32f05bebf3881b04fbb652613bd335710fce992e473ae4c5d860066d5f1
    5535bcd1f1c2acd113354cf4232d21f040e81e072d5ffaa444cc624c262eb96
```

ded70ebe55483b60d23c4def013fb9d349909d9bfa155d57df150c34472ca11
a269e2fe47cd41e1254e5ed9f09afb7d1c3bcf5fcc256017b97947d25de766c
4f0acd38362
- 0005059bb7481ed568c5abcabb533404e464b381a4e4874c1e7bcb1058183
f3018b905bebf3881b04fbb652613bd335710fce992e473ae4c5d860066d5f1
5535bcd1f1c2acd113354cf4232d21f040e81e072d5ffaa444cc624c262eb96
ded70ebe5a7d2b62940f03fd3d0c4a20a323c8758a4e3576c92d00156dc1f2d
2ff9ebe900d5d2e6ecbb6a97cdbf8f185264264dd303558815d9308d61e567f
3df9b274bbb

A.4. Generic Token Batch Issuance

The test vector below lists the following values:

* issuance: An array of parameters required to generate TokenRequest batched in the current test vector. This is sharded by a parameter type which is the protocol token type, represented as a hexadecimal string. Depending on the type, issuance contains different information

  type 0x0001 - skS: The Issuer Private Key, serialized using SerializeScalar from Section 2.1 of [OPRF] and represented as a hexadecimal string. - pkS: The Issuer Public Key, serialized according to the encoding in [RFC9578], Section 8.2.1. - token_challenge: A randomly generated TokenChallenge structure, represented as a hexadecimal string. - nonce: The 32-byte client nonce generated according to [RFC9578], Section 5, represented as a hexadecimal string. - blind: The blind used when computing the OPRF blinded message, serialized using SerializeScalar from Section 2.1 of [OPRF] and represented as a hexadecimal string. - token: The output Token from the protocol, represented as a hexadecimal string.

  type 0x0002 - skS: The PEM-encoded PKCS#8 RSA Issuer Private Key used for signing tokens, represented as a hexadecimal string. - pkS: The Issuer Public Key, serialized according to the encoding in [RFC9578], Section 8.2.2. - token_challenge: A randomly generated TokenChallenge structure, represented as a hexadecimal string. - nonce: The 32-byte client nonce generated according to [RFC9578], Section 6, represented as a hexadecimal string. - blind: The blind used when computing the blind RSA blinded message, represented as a hexadecimal string. - salt: The randomly generated 48-byte salt used when encoding the blinded token request message, represented as a hexadecimal string. - token: The output Token from the protocol, represented as a hexadecimal string.

type 0x0005 - skS: The Issuer Private Key, serialized using SerializeScalar from Section 2.1 of [OPRF] and represented as a hexadecimal string. - pkS: The Issuer Public Key, serialized according to the encoding in [RFC9578], Section 8.2.1. - token_challenge: A randomly generated TokenChallenge structure, represented as a hexadecimal string. - nonce: The 32-byte client nonce generated according to [RFC9578], Section 5, represented as a hexadecimal string. - blind: The blind used when computing the OPRF blinded message, serialized using SerializeScalar from Section 2.1 of [OPRF] and represented as a hexadecimal string. - token: The output Token from the protocol, represented as a hexadecimal string.

* token_request: The AmortizedBatchTokenRequest message constructed according to Section 6.1, represented as a hexadecimal string.

* token_response: The BatchedTokenResponse message constructed according to Section 6.2, represented as a hexadecimal string.

Note to implementers: Generic batched token is an issuance protocol that does not define a token type. You should decide which test vectors is required for your implementation. The batch for each test vector is the following

* Test vector 1: [0x0001]

* Test vector 2: [0x0002]

* Test vector 3: [0x0001, 0x0001]

* Test vector 4: [0x0002, 0x0002]

* Test vector 5: [0x0001, 0x0002]

* Test vector 6: [0x0001, 0x0002]

* Test vector 7: [0x0002, 0x0001]

* Test vector 8: [0x0001, 0x0002, 0x0005, 0x0002]

```
// Test vector 1:
issuance:
  - type: 0001
    skS: 39b0d04d3732459288fc5edb89bb02c2aa42e06709f201d6c518871d
    518114910bee3c919bed1bbffe3fc1b87d53240a
    pkS: 02d45bf522425cdd2227d3f27d245d9d563008829252172d34e48469
    290c21da1a46d42ca38f7beabdf05c074aee1455bf
    token_challenge: 0001000e6973737565722e6578616d706c65205de58a
```

```
      52fcdaef25ca3f65448d04e040fb1924e8264acfccfc6c5ad451d582b3000
      e6f726967696e2e6578616d706c65
      nonce: 332897fa11779e9594b096e5cfc5e43b1405338717bf27b49e9956
      c1f212fcbf
      blind: 6572ac688f2a37a1e6b9ba7a84a6034d9cb82673723e2a2d1413de
      60ea296a7ce0ea351b6dfa6e63a1b390460567f903
      token: 0001332897fa11779e9594b096e5cfc5e43b1405338717bf27b49e
      9956c1f212fcbf501370b494089dc462802af545e63809581ee6ef57890a1
      2105c28368169514bf260d0792bf7f46c9866a6d37c3032d8714415f87f5f
      6903d7fb071e253be2f41077848f52b6bdd765ec802dadae854edff52d167
      7c444fe222146fe425e751c826b4eccf4c4983b840af2f73a07027d
  token_request: 340001f4036e7830ee395c3e0f9d63ea6791db427062f77387
  2ef64bc4a0935e4c95803558c4743f2b8626fbd655b0e2fac742e217
  token_response: 409401000103ea1ec6b484c65905806dd80e159bee70451eb
  f99e4e74059da8cb4efc1129292ebaf28a690df8f7f73dc8afe6628c48ead526d
  157aeb36848554fa0559afa23378163844098eceed1b30d73a6681a387fed082a
  933bd3597bc1f76a0a77ccf7cb65d20dc14499fb4cb97d883f7b6f5e49ef6e016
  861fff4a294a620f83d3ce26dd52f6d62cb974d0aa76c23752dc5c24

  // Test vector 2:
  issuance:
    - type: 0002
      skS: 2d2d2d2d2d424547494e20505249564154452044b45592d2d2d2d2d0a
      4d4949457651494241444414e42676b71686b69473977304241514546414 15
      343424b63776767536a41674541416f49424151444c477531726170583173
      6334420a4f6b7a38717957355379356b6f6a41303543554b66717444774e3
      8366a424b5a4f76457245526b49314c527876734d64533279613263336 16b
      4745714c756b440a556a35743561496b3172417643655844644e445034423
      25055707851436e6969396e6b492b6d6772576974444449487138613979 31
      37586e6c5079596f784f530a646f6558563835464f314a752b62397336356
      d586d34516a7551394559614971383371724450567a50335758712b524e4d
      6363793232696867636 24c766d42390a6a41355334475666325a6c7478595
      4736f4c364872377a58696a4e39463748627165676f753967654b524d5846
      45352f2b4a3956595a634a734a624c756570480a544f72535a4d4948502b5
      358514d4166414f454a4547426d6d4430683566672f43473475676a79486e
      4e51383733414e4b6a55716d367657457441387251 4c620a4530742b496c7
      06641674d4241414543676745414c7a4362647a69316a506435384d6b562b
      434c6679665351322b7266486e7266724665502f566344787275690a32703
      16153584a596962653645532b4d622f4d4655646c485067414c7731785134
      576572663663364443736 86c6c784c5753563847734273766338 6f3647503
      20a6359366f77704244776362616847 4b556b5030456b62395330584c4a57
      634753473561556e484a585237696e7834635a6c666f4c6e7245165366 85
      578734d710a6230644878644844424d644766565777674b6f6a4f6a70532f
      39386d4555793756422f3661326c7265676c766a632f326e4b434b7459373
      744376454716c47460a787a414261577538364d435a342f5131334c762b42
      6566627174493973715a5a776a726455685148385643787279325156 4d515
      751696e57684174364d7154340a53425354726f6c5a7a7772716a65384d50
      4a393175614e4d6458474c63484c49323673587a76374b53514b426751447
```

```
663777350555576413 95a325a583958350a6d49784d54424e6445467a5662
5550754b4b413179576e31554d444e63556a71682b7a652f376b337946786
b68305146331627136306 54c393047495369414f0a354b4f574d39454b6f
2b7841513262614b314d664f5931472b386a7a42585570427339346b35335
3383879586d4b366e796467763730424a385a6835666b55710a5732306f53
62686b686a5264537a48326b52476972672b5553774b426751445a4a4d6e7
279324578612f3345713750626f737841504d69596e6b354a415053470a79
327a305a375455622b7548514f2f2b78504d376e433075794c494d44396c6
1544d48776e3673372f4c62476f455031575267706f59482f4231346b2f52
6e360a667577524e3632496f397463392b41434c74554237674476179332
b675277597453433262356564386c4969656774546b656130683075445352
7841745673330a6e356b796132513976514b4267464a75467a4f5a742b746
7596e576e5155456757385030 4f494a45484d45345554644f637743784b72
48527239334a6a7546320a453377644b6f546969375072774f59496f614a5
468706a50634a62626462664b792b6e7351703159477639776 44a724d6156
774a6376497077563676315570660a56744c61646d316c6b6c76707173364
74e4d386a6e4d30587833616a6d6d6e666557397947584535706 84d727a4c
4a6c394630396349324c416f4742414e58760a756756587270326273543 16
f6b643675536142736770 4a6a5065774e526433635a4b397a306153503144
544131504e6b7065517748672f2b36665361564f487a0a794178447339683
55272627852614e6673542b7241554837783153594456565159564d685552
62546f5a6536472f6a716e544333664e6648563178745a666f740a306c6f4
d4867776570362b53494d436f6565325a6374755a5633326c634961663972
62484f633764416f47416551386b3853494c4e4736444f413331544535500
a6d3031414a49597737416c5233756f2f524e61432b78596450553354736b
75414c78786944522f57734c455142436a6b46576d6d4a41576e515544746
26e594e0a536377523847324a36466e7245437462747973733574156476f
6f465a6e636d504c50386c784c79626c534244454c79615a762f624173506
c4d4f39624435630a4a2b4e534261612b6f694c6c31776d4361354d43666c
633d0a2d2d2d2d2d454e442050524956415445204b45592d2d2d2d2d0a
pkS: 30820152303d06092a864886f70d01010a3030a00d300b0609608648
016503040202a11a301806092a864886f70d010108300b060960864801650
3040202a2030201300382010f003082010a0282010100cb1aed6b6a95f5b1
ce013a4cfcab25b94b2e64a23034e4250a7eab43c0df3a8c12993af12b111
908d4b471bec31d4b6c9ad9cdda90612a2ee903523e6de5a224d6b02f09e5
c374d0cfe01d8f529c500a78a2f67908fa682b5a2b430c81eaf1af72d7b5e
794fc98a3139276879757ce453b526ef9bf6ceb99979b8423b90f4461a22a
f37aab0cf5733f7597abe44d31c732db68a181c6cbbe607d8c0e52e0655fd
9996dc584eca0be87afbcd78a337d17b1dba9e828bbd81e291317144e7ff8
9f55619709b096cbb9ea474cead264c2073fe49740c01f00e109106066983
d21e5f83f086e2e823c879cd43cef700d2a352a9babd612d03cad02db134b
7e225a5f0203010001
token_challenge: 0002000e6973737565722e6578616d706c65205de58a
52fcdaef25ca3f65448d04e040fb1924e8264acfccfc6c5ad451d582b3000
e6f726967696e2e6578616d706c65
nonce: 215c56ebf1bce65aff6f99833be25082a9f308f4d39a4cf9b0fd44
18a9ca1882
blind: 8e023c5f212462a34c03cc59b7316c2f5901bf56695d6e6f05c3f6
```

```
      08ec588da686dfd48d200c6953c75b69cda3e19ff48556c23c32dbebc39f7
      2b5fd8cfd8230af807c0dec3eb86b7bbe490767ef6056aeb828b2316fd4b6
      70d087ddde5ace55f6ef2e78b76bb83a79ed462ae150a923d19772a6c8de4
      7e376626c25732e7a66de5ca92a63f93b4dcd7ecd680bb3fec230951df790
      8c253556af29409dd3c037d5cb16b0861b723d1839090e882463ac10e7cf3
      a78c12e7664c68aec7a33fde219ab7a0068d32265bfc211476a462c034209
      2b08f96804e0b83a3ebe93b516db9ddde3d97344a52f3d90302c2e136a39b
      660f035db44543c15348fd91da04d01
      token: 0002215c56ebf1bce65aff6f99833be25082a9f308f4d39a4cf9b0
      fd4418a9ca1882820fc64e2630a0d5166c36696b663ff34518338263383ec
      92b3347ea30bddae4ca572f8982a9ca248a3056186322d93ca147266121dd
      eb5632c07f1f71cd27082bbead86719e39ee60b224ba39aed396e7b28cfb9
      cbbd8b654887fc04921f76dc92ef72cb47650cd95bebd277162ab0ea03e60
      ddf9cced0d8e076ad065e29a04ef8c69fd880a5cf58db7b3f9153ee5a7382
      685d1b4d1712ee944a92fae4fba32ff4d9288a37f6db1eb29ea7cfc9ea2cc
      b4aa1c729c0b4b95c5a40e66d9b9f8fee7d87ff8e8513b7ac1e934b74d68b
      8551e102fbd1fb0404bc1904ada8684aa0afca6275877b33224cd15ad1b77
      1ba9af7821385017ca34e2eb9644a88c204675cbb1bf3b7cd7cdf9055b3b3
      77057faec7a36e81652e6d0654280c017723e878f0c9d993bace51a51685c
      62ff22f0ea37c244a6478077e914539e65f95372e4cf
   token_request: 4103000208a84566ca40ac42d01bc0e0ad10d2d8f9bf45bb30
   326ce3a3ad0f2b56589c1e9260679876a1271c83fbb5dfa9433c72a0a6362dbee
   06f96f3e3591c3ca8dad240e1c9696fa7a41b79306a868cd1cfe66432129ab209
   02be6a8214d11f8863a74b2ece62de4fc75b4968b87216471e6b719cf6c91c99a
   bb83bc98fabae802aa09868b1bdae58a73023bdb83c54d6bebfabbef837c9d4ef
   88a7a0e742e32a860e05cb798b4d09d8eb1336da49d8d83fb619ae556617246b6
   24b5a0fd55f16e27150c96b6b4d645d897d04443bfb5f519eabada7b8b4d9013e
   8f6f954356231dfea1e8e7121eb52a5157fe10381689b7f343cd4380e77727ac9
   6a126f097b5f79758
   token_response: 410301000212093795bb6bde21df488d56d18ac4efc280d6a
   493528fb180ff6204ad2c2e6396ad19c348103c7adee2c254bb4ee4f0c0015ac0
   70bf41d23a78856880f1b506ba28ca3d370e262216e68ffdc6be57bcb0e03d7c3
   e112b63a5695dbbfb220ccdd68a601d829821ffa19b5ddb2da6da3f71e308d702
   53f43b7b52d2739f2380ad5150be14db16ef39ca9c475255b0879ddee0f1147e9
   230e12e20b5ca7e2069e9ed87db7507f3eb78d9fbf2a957f8410cc80114e9006d
   1d6c61d3712b04935d62356b0e7540b10189394eed8206e65631e77e7f75ba076
   8bdbace3ffae1bc70ca86303c3e0d3268bf4dbe3225a618926cf3f2f4ca2c80a9
   a2f95bf638699792b8

   // Test vector 3:
   issuance:
     - type: 0001
       skS: 39b0d04d3732459288fc5edb89bb02c2aa42e06709f201d6c518871d
       518114910bee3c919bed1bbffe3fc1b87d53240a
       pkS: 02d45bf522425cdd2227d3f27d245d9d563008829252172d34e48469
       290c21da1a46d42ca38f7beabdf05c074aee1455bf
       token_challenge: 0001000e6973737565722e6578616d706c65205de58a
       52fcdaef25ca3f65448d04e040fb1924e8264acfccfc6c5ad451d582b3000
```

```
      e6f726967696e2e6578616d706c65
      nonce: 79f68dbc610a490d940367f0de8a008c5f429c535dd758afa59965
      d7be6d8753
      blind: 4581461cfd525cd59babb8abbcacafd69c8a6da3fdeffc209be423
      23d2884c09c15beef67287112bec9f674f6e3ef523
      token: 000179f68dbc610a490d940367f0de8a008c5f429c535dd758afa5
      9965d7be6d8753501370b494089dc462802af545e63809581ee6ef57890a1
      2105c28368169514bf260d0792bf7f46c9866a6d37c3032d8714415f87f5f
      6903d7fb071e253be2f4a18606ab08b9d569d144f8944655cda17c6ec74d2
      4a11ebd7622a56d551e223a776fa9650dc2a4a00e083444160e27e5
    - type: 0001
      skS: 39efed331527cc4ddff9722ab5cd35aeafe7c27520b0cfa2eedbdc29
      8dc3b12bc8298afcc46558af1e2eeacc5307d865
      pkS: 038017e005904c6146b37109d6c2a72b95a183aaa9ed951b8d8fb1ed
      9033f68033284d175e7df89849475cd67a86bfbf4e
      token_challenge: 0001000e6973737565722e6578616d706c6500000e6f
      726967696e2e6578616d706c65
      nonce: 5d0d763f6e9da102fdb9e1a7f95a1b096391f02ac87f65888233e9
      415df05c56
      blind: fdef8385c0ea23299a8b52b59b23ffa9f1a0f25c3a4c93d9579237
      2910091cd47ec89b14321b3e00a8d3eb0949e7bbd6
      token: 00015d0d763f6e9da102fdb9e1a7f95a1b096391f02ac87f658882
      33e9415df05c56c994f7d5cdc2fb970b13d4e8eb6e6d8f9dcdaa65851fb09
      1025dfe134bd5a62a116477bc9e1a205cca95d0c92335ca7a3e71063b2ac0
      20bdd231c66097f12333a13b1c96dbe522e6e94e0ecba8c3abad7fac579bd
      dae7233e8f0ad13192b3c895fc7f4229e9156314a71c338ff74baba
  token_request: 40680001f403f509ce89b5e1012f47b34af3a33a120556a5f9
  771764c33c8bf330076cfd668fc09d0bd7a740f74852d258cbb1a8b49a0001330
  27cd2c1b2552ae7bf9282c4eed9aaf03a7e99969ad4af29e615be378f9d944006
  2bdf296f39ec999ab9c7a94f62f9df7a
  token_response: 41280100010229c3174c22f284bf32ea4f5c2e76b4b969be9
  e5d8e163861e77eb673ce0c7af96c2745064749fd59edbe9b4b4e7e80e522d72d
  28882d9b60434ab5c7ed142d8da3465291a04dcb1c3ea1a8444dcb09206a4f3ee
  92ac498753ec042da0fd72602c679bf7a994f9fbca0fae57740fd47772e237569
  fdcfa587874f0e1a538abc3333f8ee486809347eef1e49a83381317201000103b
  027ff354e5b1728d6dae0de169816ad92912d96a057e80363b697e253a0a74aad
  1513efbeff7356e75c6989863191af7be62c4c0251b441088a2221e96f2273222
  33e1b4e3785ddc98bd3f310f69a51e8268478bc080fac60032c63da2332f230e3
  f04497959469593e2fac77cd6d58dd3e59081d1279f87ea9cd81c87e38d218093
  590d6ec8f8caaf4581a9fece56b

  // Test vector 4:
  issuance:
    - type: 0002
      skS: 2d2d2d2d2d424547494e20505249564154452045592d2d2d2d2d0a
      4d4949457651494241444414e42676b71686b69473977302415145464141 5
      343424b63776767536a41674541416f49424151444c477531726170583173
      6334420a4f6b7a387179573553793566b6f6a41303543554b66717444774e3
```

```
8366a424b5a4f76457245526b49314c527876734d6453327961326333616b
4745714c756b440a556a35743561496b3172417643655844644e445034423
25055707851436e6969396e6b492b6d67725769744444494871386139793 1
37586e6c5079596f784f530a646f6558563835464f314a752b62397336356
d586d34516a7551394559614971383371724450567a50335758712b524e4d
6363793232696867636 24c766d42390a6a41355334475666325a6c7478595
4736f4c364872377a58696a4e39463748627165676f753967654b524d5846
45352f2b4a3956595a634a734a624c756570480a544f72535a4d4948502b5
358514d4166414f454a4547426d6d4430683566672f43473475676a79486e
4e51383733414e4b6a55716d3676574574413872514c620a4530742b496c7
06641674d4241414543676745414c7a4362647a69316a506435384d6b562b
434c6679665351322b7266486e7266724665502f566344787275690a32703
16153584a596962653645532b4d622f4d4655646c485067414c7731785134
576572663663364443736 86c6c784c575356384773427376633 86f3647503
20a6359366f77704244776362616847 4b556b5030456b62395330584c4a57
634753473561556e484a585237696e7834635a6c666f4c6e7245516536685
578734d710a6230644878644844424d644766565777674b6f6a4f6a70532f
39386d4555793756422f3661326c7265676c766a632f326e4b434b7459373
744376454716c47460a787a414261577538364d435a342f5131334c762b42
6566627174493973715a5a776a726455685148385643787279325 1564d515
751696e57684174364d7154340a53425354726f6c5a7a7772716a65384d50
4a393175614e4d6458474c63484c49323673587a76374b53514b426751447
6637773505555764 1395a325a583958350a6d49784d54424e6445467a5662
5550754b4b413179576e31554d444e63556a71682b7a652f376b337946786
b6830514633316271363065 4c393047495369414f0a354b4f574d39454b6f
2b7841513262614b314d664f5931472b386a7a4258557042733934 6b35335
3383879586d4b366e79646776373042 4a385a6835666b55710a5732306f53
62686b686a5264537a48326b52476972672b5553774b426751445a4a4d6e7
279324578612f3345713750626f737841504d69596e6b354a415053470a79
327a305a375455622b7548514f2f2b78504d376e433075794c494d44396c6
1544d48776e3673372f4c62476f455031575267706f59482f4231346b2f52
6e360a667577524e3632496f397463392b41434c7455423767447617933 2
b675277597453433262356564386c4969656774546b656130683075445352
7841745673330a6e356b796132513976514b4267464a75467a4f5a742b746
7596e576e5155456757385030 4f494a45484d45345546446f637743784b72
48527239334a6a7546320a453377644b6f546969375072774f59496f614a5
468706a50634a62626462664b792b6e7351703159477639776 44a724d6156
774a6376497077563676315570660a56744c61646d316c6b6c76707173364
74e4d386a6e4d30587833616a6d6d6e6665573979475845357068 4d727a4c
4a6c394630396349324c416f4742414e58760a756756587270326273543 16
f6b6436755361427367704a6a5065774e526433635a4b397a306153503144
544131504e6b7065517748672f2b36665361564f487a0a794178447339683
55272627852614e6673542b72415548377831535944565651595 64d685552
62546f5a6536472f6a716e544333664e6648563178745a666f740a306c6f4
d4867776570362b53494d436f6565325a6374755a5633326c634961663972
62484f633764416f47416551386b3853494c4e4736444f413331544535500
a6d3031414a49597737416c5233756f2f524e61432b78596450553354736b
75414c78786944522f57734c455142436a6b46576d6d4a41576e515544746
```

```
      26e594e0a536377523847324a36466e72454374627479733733574156476f
      6f465a6e636d504c50386c784c79626c534244454c79615a762f624173506
      c4d4f39624435630a4a2b4e534261612b6f694c6c31776d4361354d43666c
      633d0a2d2d2d2d2d454e442050524956415445204b45592d2d2d2d2d0a
      pkS: 30820152303d06092a864886f70d01010a3030a00d300b0609608648
      016503040202a11a301806092a864886f70d010108300b060960864801650
      3040202a203020130038201 0f003082010a0282010100cb1aed6b6a95f5b1
      ce013a4cfcab25b94b2e64a23034e4250a7eab43c0df3a8c12993af12b111
      908d4b471bec31d4b6c9ad9cdda90612a2ee903523e6de5a224d6b02f09e5
      c374d0cfe01d8f529c500a78a2f67908fa682b5a2b430c81eaf1af72d7b5e
      794fc98a3139276879757ce453b526ef9bf6ceb99979b8423b90f4461a22a
      f37aab0cf5733f7597abe44d31c732db68a181c6cbbe607d8c0e52e0655fd
      9996dc584eca0be87afbcd78a337d17b1dba9e828bbd81e291317144e7ff8
      9f55619709b096cbb9ea474cead264c2073fe49740c01f00e109106066983
      d21e5f83f086e2e823c879cd43cef700d2a352a9babd612d03cad02db134b
      7e225a5f0203010001
      token_challenge: 0002000e6973737565722e6578616d706c65205de58a
      52fcdaef25ca3f65448d04e040fb1924e8264acfccfc6c5ad451d582b3000
      e6f726967696e2e6578616d706c65
      nonce: e7615e63a25a89c13ad49ce0249c8d75ec481dc95e005454563ede
      8c6b0f1f46
      blind: 30465e67d38960c99589a56a8b965191aa709b91fd2a56c101120b
      4453e9a561f2bd041d49ec895684018fa6aba34ab3dd2137777f9e9829a0a
      0d0a678a06e16a3aed47a7e9652ff99fafb5e86a6807f8ddf5b50fcde11b4
      bf7dac7ee5e4f200776eba2c33d6eb187ccb109999e8c9c67595b5464f1ed
      2948b19c04689fe9c29c6863208a2e15b70b0e456ab4f8369569bdb14a903
      bacde57b6ce0bfa21ada35d52c4fea231b40c26254d5130b41f71a21eadff
      dc60e41ab3c072236cb2d1926cb21eb873bb66365a72d619a58cfdfa963d3
      8cdf4cb54db1fc2b42731ba207ad9a897092e8bfc9be2a1f4551da3452a22
      926cc98971da1e2d6287e2c8c013006
      token: 0002e7615e63a25a89c13ad49ce0249c8d75ec481dc95e00545456
      3ede8c6b0f1f46820fc64e2630a0d5166c36696b663ff34518338263383ec
      92b3347ea30bddae4ca572f8982a9ca248a3056186322d93ca147266121dd
      eb5632c07f1f71cd2708baa04e4e9511d5e1b49ad181913b67498a06d54ee
      d0bb7ad9a8caa4a1c46dfabc6dc456b1be1fa49d8a630925cb124b3dcf38e
      4a7fef67bc1cb8b25c4d1f78e341fe7c5f03d7e8ef193602a79d9c11cdb9c
      758e86d6a2ce5d6bbc6ebab3c1ac426202300a752f9adaf8f0ce3ff60fc7a
      ce0d5a2fdcc29f0161495d8953aa7fd6c27c94ca3609b4981cf07f9e2d006
      74b5e7ee0701925b7845a7702d9193178594a659eccebfcd12a505bd28c58
      efdee3dc6b971339dfa24b83f0a24e3197d51218175bf5dcdf7ae6d03a8d2
      74734b40af38680a2bdfd375febd2fb436f00f66c709f89996ad4bd8b28f9
      2b8110036f4df03f3cbf7b8673c37db31f925ea69c15
    - type: 0002
      skS: 2d2d2d2d2d424547494e20505249564154452045592d2d2d2d2d0a
      4d4949457651494241444144e42676b71686b6947397730424151454641415
      343424b63776767536a41674541416f49424151444c477531726170583173
      6334420a4f6b7a38717957355379356b6f6a41303543554b66717444774e3
      8366a424b5a4f76457245526b49314c527876734d6453327961326333616b
```

```
4745714c756b440a556a35743561496b3172417643655844644e445034423
25055707851436e6969396e6b492b6d6772576974444449487138613979 31
37586e6c5079596f784f530a646f6558563835464f314a752b62397336356
d586d34516a7551394559614971383371724450567a50335758712b524e4d
6363793232696867636 24c766d42390a6a4135533447566632 5a6c7478595
4736f4c364872377a58696a4e39463748627165676f753967654b524d5846
45352f2b4a3956595a634a734a624c756570480a544f72535a4d4948502b5
358514d4166414f454a4547426d6d4430683566672f43473475676a79486e
4e51383733414e4b6a55716d3676574574413872514c620a4530742b496c7
06641674d4241414543676745414c7a4362647a69316a506435384d6b562b
434c6679665351322b7266486e7266724665502f566344787275690a32703
16153584a596962653645532b4d622f4d4655646c485067414c7731785134
576572663663364443736 86c6c784c575356384773427376338 6f3647503
20a6359366f77704244776362616847 4b556b5030456b62395330584c4a57
634753473561556e484a585237696e7834635a6c666f4c6e7245516536685
578734d710a6230644878644844424d644766565777674b6f6a4f6a70532f
39386d4555793756422f3661326c7265676c766a632f326e4b434b7459373
744376454716c47460a787a414261577538364d435a342f5131334c762b42
6566627174493973715a5a776a726455685148385643787279325156 4d515
751696e57684174364d7154340a53425354726f6c5a7a7772716a65384d50
4a393175614e4d6458474c63484c49323673587a76374b53514b426751447
6637773505555764139 5a325a583958350a6d49784d54424e6445467a5662
5550754b4b413179576e31554d444e63556a71682b7a652f376b337946786
b6830514633316271363 0654c393047495369414f0a354b4f574d39454b6f
2b7841513262614b314d664f5931472b386a7a4258557042733934 6b35335
3383879586d4b366e796467763730424a385a6835666b55710a5732306f53
62686b686a5264537a48326b52476972672b5553774b426751445a4a4d6e7
279324578612f3345713750626f737841504d69596e6b354a415053470a79
327a305a375455622b7548514f2f2b78504d376e433075794c494d44396c6
1544d48776e3673372f4c62476f455031575267706f59482f4231346b2f52
6e360a667577524e3632496f397463392b41434c7455423767447617 9332
b675277597453433262356564386c4969656774546b656130683075445352
7841745673330a6e356b796132513976514b4267464a75467a4f5a742b746
7596e576e5155456757385030 4f494a45484d4534555464 4f637743784b72
48527239334a6a7546320a453377644b6f546969375072774f59496f614a5
468706a50634a62626462664b792b6e7351703159477639776 44a724d6156
774a6376497077563676315570660a56744c61646d316c6b6c76707173364
74e4d386a6e4d30587833616a6d6d6e6665573979475845357068 4d727a4c
4a6c394630396349324c416f4742414e58760a756756587270326273543 16
f6b6436755361427367704a6a5065774e526433635a4b397a306153503144
544131504e6b7065517748672f2b36665361564f487a0a794178447339683
55272627852614e6673542b7241554837783153594456565159564d685552
62546f5a6536472f6a716e544333664e6648563178745a666f740a306c6f4
d4867776570362b53494d436f6565325a6374755a5633326c634961663972
62484f633764416f47416551386b3853494c4e4736444f413331544535500
a6d3031414a49597737416c5233756f2f524e61432b7859645055335473 6b
75414c78786944522f57734c455142436a6b46576d6d4a41576e515544746
26e594e0a536377523847324a36466e7245437462747973733574156476f
```

```
      6f465a6e636d504c50386c784c79626c534244454c79615a762f624173506
      c4d4f39624435630a4a2b4e534261612b6f694c6c31776d4361354d43666c
      633d0a2d2d2d2d2d454e442050524956415445204b45592d2d2d2d2d0a
      pkS: 30820152303d06092a864886f70d01010a3030a00d300b0609608648
      016503040202a11a301806092a864886f70d010108300b060960864801650
      3040202a203020130038201 0f003082010a0282010100cb1aed6b6a95f5b1
      ce013a4cfcab25b94b2e64a23034e4250a7eab43c0df3a8c12993af12b111
      908d4b471bec31d4b6c9ad9cdda90612a2ee903523e6de5a224d6b02f09e5
      c374d0cfe01d8f529c500a78a2f67908fa682b5a2b430c81eaf1af72d7b5e
      794fc98a3139276879757ce453b526ef9bf6ceb99979b8423b90f4461a22a
      f37aab0cf5733f7597abe44d31c732db68a181c6cbbe607d8c0e52e0655fd
      9996dc584eca0be87afbcd78a337d17b1dba9e828bbd81e291317144e7ff8
      9f55619709b096cbb9ea474cead264c2073fe49740c01f00e109106066983
      d21e5f83f086e2e823c879cd43cef700d2a352a9babd612d03cad02db134b
      7e225a5f0203010001
      token_challenge: 0002000e6973737565722e6578616d706c6500000e6f
      726967696e2e6578616d706c65
      nonce: d17d88fb4f63d0b3b38d1159bef67ac6d60f649aba512b8e382d49
      7530727577
      blind: 4e192daf9edea831f3c82a274c5648d758f6930991334d820a2a24
      e96101023a86de1d18836222c42dcb0eb39a9153ada0b4eea7d3395d55114
      d8ec972655b47bebb3e66f72f6bfadb5cb976c98907fea985eb13bd5675c9
      c39144381d0b0038c12f6ff9fd598ab8eaef47a878da4fa10d3bd3e4c7e86
      a60ce15e07f5de0501c65d653d20f6dd83763f152ec7beecba6ca51914ddf
      00f79f5143d6854bdefd3032ced824066b8586f6e5d3ecafcb268c99c103c
      d4fab99eeb3afbe550690172ebe09edb533fec7095c357180439c2c32f8af
      85ba77b85cba091f3eae542d01a3de3cdabf57439fe6f41fb2d3c15c23a5b
      c23b3be8fe0140944a76760a7b38301
      token: 0002d17d88fb4f63d0b3b38d1159bef67ac6d60f649aba512b8e38
      2d49753072757711e15c91a7c2ad02abd66645802373db1d823bea80f08d4
      52541fb2b62b5898bca572f8982a9ca248a3056186322d93ca147266121dd
      eb5632c07f1f71cd2708bb7df188c0ed5642312cb5152735825a75d982d17
      a705843b9dc59847cae233b3e69a8500978d1fb360794c4223fcf7483e844
      a1db3e316656456e2d06262e0b051f22e91b4e912cee082b87b40e01a5b70
      734de93f739e6c0abf05a935a8de4bddecb977bd2dbb27f9680ec61068f8d
      c09bcce8f82885a1820275e0a049e566a73b8b8f6050d34866281fb58761c
      7560f0ad32899ad8545d8e633642364155aa6fb397547fb9f1bbfb0bcdfa3
      401750edc31e6f42cb64a931b87032f51cf22d201d8c477135644044b9003
      814117e9313cbd45eb76fcd89f5af4200fdacde27fef511279616748b9ddd
      7fa23e6937047d0ae33ce0572430b9fb793788c1ebbe
   token_request: 4206000208bb3699eb03b73b43d87960140ba6e77a9a18ab6a
   9492176c420096872a88b15b4bbda37f43bb22ff0e6c730fcda255c4158ce10c8
   bb66995a67b2fe1992059cf6d686e1e696e8a6375bb6e77d73570cf30fadf94f4
   5f5131550bcf556722c9b62912766b17a828ea69fa3e048d5d46ac70bac8cdd8d
   86330c719e734874c00fcf23dd25a1294c9610689e59cbf0805b5d9adef2ffa5a
   9e31902bc6b8dafb39b0aad2c520cbc9c1c55696f9e96a5db2b32dbbd2b4f75c7
   481499a31ae2df1cc879475bd7ce402ee5dbaf624d87bb7c88f5b243c4094004b
   b145f71f6d98da7899ff566398468b99e41ce25f1a88ed49fb4ef26d817d6a152
```

```
   0ec0aaea6bf0d93360002089cfb2feafef5b7bf534a945daa929e87756bc8a997
   2202995b10eebfd476c81fdede8a017513ee84259fcd475330f2379d5d7b578bf
   181f9df9246fdf4b594c1d989650cde9e040c3aac7c476c2e6c87d20a3381ae04
   55e21e03b6957670219d7af3a295c932ad7735dbfd43b7c464ca82d293d1910b2
   5c2d6f293af2f46b30396de4f009e0e2ba05f431802b2d4b5fbd8e17a01b58757
   1e06382b5d26895b53327ce2ab9055e0825cf297909f6d3993a516dc9fc69824a
   7361deaadc3c7a133c129fd93f11906b4b2f88170c80fc5e6596c3ee550da51c1
   b69835f4f127a71f5d44a94d954fa056c6bc4e5ea1f49f4175eebae188a85a2e6
   80291fd4f441377
   token_response: 420601000206b0e6922469eb5587c12bacfda4ff18a732049
   b35fae442431344d136ee8be0c1080b2ad2e0ae379ac39abe3aacdb88b52614ed
   9c0c1aa3ae10edd9cdd1f776e67c3aeebcc0656cd4c4b109861904b48e9b902f5
   84565125dd97f7ed013b12f5412fbc3378234a904f1621a5b67790f6f677bd6d4
   682ab5285a342ed4d4a508360ed9b73907451e6690e88313d4f132034a1f76916
   aeceb43051b5f294303bb03de91c9b12022b1493f3b8019219134d214ab09906d
   d395e282f255940a411eda4cf0b8ab2121f802b62ce891d84fe3b2c5b32e00fef
   88a8756ad015ded4a3dcaf45657597f0677e792c250bdfe809edbb567d526e8cd
   9e9c94ad67c0486139010002baa9791c04572ce81c4b02909cafd1dc248a0ea53
   b6fa3237b98ddc3fb970bae23733d980846fd7f53a7b90655939678fac4353604
   1bfb99dd4891add3bbd7cd05d363e5142b9917ec0c195724c62d7ae6b7e657388
   70ad9ccaea0e7415cb268ba21acc141939e4853f9f5e1fab60edad58eee3eabfc
   a317a581534f3666aed5420e984dd74c655f32611315e0af4bb1d37165bd20a55
   a0c19b1e930516d83d1c2841e382aff16de515cce34cdb1191809e2cc8678b087
   539e085942be0e50f6e17d81af48c9bc94ffe4f8a6311a8537c1ed911ad88fb86
   1fac00cda3fedfab48fbb073aa05e544acc976ff6368364f5b0c6245e0a7167fb
   1af485fc90f73729

   // Test vector 5:
   issuance:
     - type: 0001
       skS: 39b0d04d3732459288fc5edb89bb02c2aa42e06709f201d6c518871d
       518114910bee3c919bed1bbffe3fc1b87d53240a
       pkS: 02d45bf522425cdd2227d3f27d245d9d563008829252172d34e48469
       290c21da1a46d42ca38f7beabdf05c074aee1455bf
       token_challenge: 0001000e6973737565722e6578616d706c65205de58a
       52fcdaef25ca3f65448d04e040fb1924e8264acfccfc6c5ad451d582b3000
       e6f726967696e2e6578616d706c65
       nonce: 0d399a51a32286661e8ecd6b601cccace4f45e8f41b05d6fae4782
       6d46142139
       blind: 43dfc280832318de5d86c6626303628b13b62670d8b134ffd008e1
       226df79dccbeaaf3ac555a9f544db50497757a0a2a
       token: 00010d399a51a32286661e8ecd6b601cccace4f45e8f41b05d6fae
       47826d46142139501370b494089dc462802af545e63809581ee6ef57890a1
       2105c28368169514bf260d0792bf7f46c9866a6d37c3032d8714415f87f5f
       6903d7fb071e253be2f429a429ebcef6ada26a201fdbc171f7c2739590085
       581237586e468660f6fdeec5ecd5e39cb3c908d1312a8baf8484450
     - type: 0002
       skS: 2d2d2d2d2d424547494e20505249564154455204b45592d2d2d2d2d0a
```

```
4d4949457651494241444 14e42676b71686b6947397730424151454641415
343424b63776767536a41674541416f49424151444c477531726170583173
6334420a4f6b7a3871795735537935 6b6f6a41303543554b66717444774e3
8366a424b5a4f76457245526b49314c527876734d6453327961326333616b
4745714c756b440a556a35743561496b3172417643655844644e445034423
25055707851436e6969396e6b492b6d67725769744444494871386139793 1
37586e6c5079596f784f530a646f6558563835464f314a752b62397336356
d586d34516a7551394559614971383371724450567a50335758712b524e4d
6363793232696867636 24c766d42390a6a41355334475666325a6c7478595
4736f4c364872377a58696a4e3946374862716567 6f753967654b524d5846
45352f2b4a3956595a634a734a624c756570480a544f72535a4d4948502b5
358514d4166414f454a4547426d6d4430683566672f43473475676a79486e
4e51383733414e4b6a55716d3676574574413872514c620a4530742b496c7
06641674d4241414543676745414c7a4362647a69316a506435384d6b562b
434c6679665351322b7266486e7266724665502f566344787275690a32703
16153584a596962653645532b4d622f4d4655646c485067414c7731785134
576572663663364443736 86c6c784c5753563847734273766338 6f3647503
20a6359366f77704244776362616847 4b556b5030456b62395330584c4a57
634753473561556e484a585237696e7834635a6c666f4c6e7245516536685
578734d710a6230644878644844424d644766565777674b6f6a4f6a70532f
39386d4555793756422f3661326c7265676c766a632f326e4b434b7459373
744376454716c47460a787a414261577538364d435a342f5131334c762b42
6566627174493973715a5a776a726455685148385643787279325 1564d515
751696e57684174364d7154340a53425354726f6c5a7a7772716a65384d50
4a393175614e4d6458474c63484c49323673587a76374b53514b426751447
6637773505555764 1395a325a583958350a6d49784d54424e6445467a5662
5550754b4b413179576e31554d444e63556a71682b7a652f376b337946786
b6830514633316271363065 4c393047495369414f0a354b4f574d39454b6f
2b7841513262614b314d664f5931472b386a7a4258557042733934 6b35335
3383879586d4b366e796467763730424a385a6835666b55710a5732306f53
62686b686a5264537a48326b52476972672b5553774b426751445a4a4d6e7
279324578612f3345713750626f737841504d69596e6b354a415053470a79
327a305a375455622b7548514f2f2b78504d376e433075794c494d44396c6
1544d48776e3673372f4c62476f455031575267706f59482f4231346b2f52
6e360a667577524e3632496f397463392b41434c7455423767 4476179332
b675277597453433262356564386c4969656774546b656130683075445352
7841745673330a6e356b796132513976514b4267464a75467a4f5a742b746
7596e576e5155456757385030 4f494a45484d45345554644f637743784b72
48527239334a6a7546320a453377644b6f546969375072774f59496f614a5
468706a50634a62626462664b792b6e7351703159477639776 44a724d6156
774a6376497077563676315570660a56744c61646d316c6b6c76707173364
74e4d386a6e4d30587833616a6d6d6e6665573979475845357068 4d727a4c
4a6c394630396349324c416f4742414e58760a7567565872703262735431 6
f6b6436755361427367704a6a5065774e526433635a4b397a306153503144
544131504e6b7065517748672f2b36665361564f487a0a794178447339683
55272627852614e6673542b7241554837783153594456565159564d685552
62546f5a6536472f6a716e544333664e6648563178745a666f740a306c6f4
d4867776570362b53494d436f6565325a6374755a5633326c634961663972
```

```
      62484f633764416f47416551386b3853494c4e4736444f413331544535500
      a6d3031414a49597737416c5233756f2f524e61432b78596450553354736b
      75414c78786944522f57734c455142436a6b46576d6d4a41576e515544746
      26e594e0a536377523847324a36466e72454374627479733733574156476f
      6f465a6e636d504c50386c784c79626c534244454c79615a762f624173506
      c4d4f39624435630a4a2b4e534261612b6f694c6c31776d4361354d43666c
      633d0a2d2d2d2d2d454e442050524956415445204b45592d2d2d2d2d0a
      pkS: 30820152303d06092a864886f70d01010a3030a00d300b0609608648
      016503040202a11a301806092a864886f70d010108300b060960864801650
      3040202a20302013003820l0f003082010a0282010100cb1aed6b6a95f5b1
      ce013a4cfcab25b94b2e64a23034e4250a7eab43c0df3a8c12993af12b111
      908d4b471bec31d4b6c9ad9cdda90612a2ee903523e6de5a224d6b02f09e5
      c374d0cfe01d8f529c500a78a2f67908fa682b5a2b430c81eaf1af72d7b5e
      794fc98a3139276879757ce453b526ef9bf6ceb99979b8423b90f4461a22a
      f37aab0cf5733f7597abe44d31c732db68a181c6cbbe607d8c0e52e0655fd
      9996dc584eca0be87afbcd78a337d17b1dba9e828bbd81e291317144e7ff8
      9f55619709b096cbb9ea474cead264c2073fe49740c01f00e109106066983
      d21e5f83f086e2e823c879cd43cef700d2a352a9babd612d03cad02db134b
      7e225a5f0203010001
      token_challenge: 0002000e6973737565722e6578616d706c65205de58a
      52fcdaef25ca3f65448d04e040fb1924e8264acfccfc6c5ad451d582b3000
      e6f726967696e2e6578616d706c65
      nonce: 1a89803678132b4328084be9547b3e1ab0b88ebc7b9e84acca4794
      7dbc6b14a7
      blind: 1c761ba8872e29390be3a2c1328b4f9ccc0012be0c2b09bf558ac0
      b334f84d0646ab2f89cca0c65f859a78b32b2407a90eec56f54c55916bdf5
      ad0dbaf5064e5899e18b282e10940f73917771058a0b1c992f679b3ed4f9b
      b8a2d6a6561e85a86e7a78a6d1345bdbf8a02d58ab92bc458852e8c961d90
      a14cae721728fd221737f711ae28b49c4b4eb6b76f8b58541630bf78f6fe3
      51c98da801d246f8b54787046610f136489cc8ca28dad8377983c3fc2e28e
      7ae09365b7516f1cba21b7a0d9ff87608c5cd91fbec89f978053512083bfb
      0adf22c74f0a96256e26c6d9f9436469972580e60a1104c9672b668910924
      17870d82eae4fab3c76caca50eaf5ac
      token: 00021a89803678132b4328084be9547b3e1ab0b88ebc7b9e84acca
      47947dbc6b14a7820fc64e2630a0d5166c36696b663ff34518338263383ec
      92b3347ea30bddae4ca572f8982a9ca248a3056186322d93ca147266121dd
      eb5632c07f1f71cd2708ad0995b4e273a9c7d825c7b2d7293a42f71221692
      5639a276b1a5c358120f6afb5a28c6319647b47ffef79dc39ba0eeb42f4cf
      22bcbbad7d774a5df9904f80c0826f12b8542291c53c20f6c6f05bed4146c
      2b09a2b5e424d4622ba40531b84d026ab202d01940c154ab47c6a9b377f28
      4462bea8a6285383efac6ea8b302e4bcb8855d133396fa2a5532a1dc3f280
      a101770d8f2e5d8142d7c573c9f9e29f160624b7c95811687f678a7994295
      695c14b1899c06f60e6a0fa04cfc6b8184e59f1f40babbf0dbbc3cb91047a
      659723c800b574cadc0491ea40f15e45a0337a3e7cd109de3b4e3517d4637
      059a9ab3c4a218e052d15479116d3c437e4962ce07c3
   token_request: 41370001f4021addfdbb3234410241c073cb66734cac677334
   930d7741cb973731f19b0e500e80dc6619d11c754b9f8909da8d2c3ca60002084
   9309ffde4f288fa5fd2e32c68aad9630adabbd51f273814d7583a27136527e8d7
```

```
   7fa89c8798e945b833ca9d7ef20233e55de142519891fea24222122feef56c7e3
   f7319f012e77e247b2ba1c9ae501196a82f8e3bb3039513c79f77bb0014e1666c
   a09113565bb88dd65729e8377dadba084c3adae744b7f0b6e7a66f7715c4677bf
   e364cf08f808eef5c607fe716a8509b00b688bb874e90badd7781c9f3e32d9178
   070103874ddbb94f7f8d44893ea97c869334f9ec54ad421fdedcbe264d4732da0
   b54ad25901895248df6cc75a70e9fc06fa1f7c9bfecabd45eec42e22239eb76f1
   765a1a5de3bcf12b5e4d8737ff8b54f911778038fd74fb8b3e4a3e3d
   token_response: 419701000103f46a70859a87727ade7ee8534c42b676c28e2
   2fa906a669f03172331cc85e1157097214f482a0744fa9d5083a85db2b208e4c0
   3bd4c9540fd5f183ec590aaeefafc849ff51c169149b653af450b53b830f587c8
   5bdf500074467db6bcd155b6657ad915e4e94d28642173be93a8c6c99a3ee2ee9
   ee46686f01d5f9b8208593240cf7db7a9cde0c79ce8187203133444701000 29e2
   15a04d99389aa9ed15f2df507d9fcb88819b989705fcb779d6af8bff5d5c56319
   0ba2267c58c49a923cd4d80277eb72d287bb224771bf2dd245018195a8eec6a6e
   e454e7f7600fa2f974a2feb8638620702332225288776a8b183bb30f251194df9
   55018bdb31cf992b8e37e8dcfee22a2dab536ed0a3c918cb74b0568b100df7ca9
   7bb15b6641819d0db806ab9bb67b295a3ecaf1cd0757659816605 1ddfed98d6d4
   30b176081e41432a4607213b1291ef2becaaa337961139bee6a57e0aa8b42d192
   bf468f4d187e72f7cedc6393720c34030fa809c62dd9b4ef79aaf7af950a284c9
   df77cfcd17f6f5eb022963ffa1d57d4394d24f3204db260dad97ce

   // Test vector 6:
   issuance:
     - type: 0001
       skS: 9e19dad32d440b14a7674143e272c830dfb4d5de61eae63c76571570
       956a88bbe66577db033d3cf043d343208436d6da
       pkS: 028ff446ea2e2fbd761a6ef7b1137bd59a760d6c65f3b82784cefc58
       43f9b9ed65cdcaaa90b293f4b0cb818a873ca17d15
       token_challenge: 0001000b497373756572204e616d6520941de0bab199
       d9a3cd01d5f58529d5cc9b1ceac6614d92ff75a36241c96439b20005612c6
       22c63
       nonce: b771dc02997c71738e631f7f52e1f786e9c80eb51e9ed54a1302fb
       f98f5b32c3
       blind: ccb1a833c28efff813ec2de76d4bd325874da893e8116d583ad3c6
       48341398560a6a2c1b64c52b4ea9ea97b4e1f24e54
       token: 0001b771dc02997c71738e631f7f52e1f786e9c80eb51e9ed54a13
       02fbf98f5b32c3c605cc17c7449af46256832938618c13b44148d3ba19c13
       5c0e992dc15463a626b2e907957aaa5def3d775fa880539bed74e2c2f8fb6
       3f80b64624844b9053737a28749068a0a33347af11be755343eb7e23bd1fb
       6b18539ae4ce776ead2c340e8ffc496583950c2672683568f78423b
     - type: 0002
       skS: 2d2d2d2d2d424547494e20505249564154452044b45592d2d2d2d2d0a
       4d4949457641494241444 14e42676b71686b6947397730424151454641415
       343424b597767675369416745414 16f4942415144312f78627745396c476a
       354a4c0a6736326e583844795035634864515739396531465a6d306738797
       24d51357742474b4746555a4f554246464f706c45774d4e726763764f6a6e
       55733351346e4c0a775a693262453067623556 4c7a6754756b587a2f32437
       64742534661557374466176755855475777702f516e325a4f51316d586345
```

```
623762574774634945397 90a512f356e5962493934654e596b50716146355
94a3871446a333447702f6865706a4a73586a4537715432363162615972 2f
5839496e306b6441366c397542384c0a5276745a614e5677546d4445686e6
1625a7a7154416c5170387633794245587 36f63456d496d35336443634c63
47494d6250387046747559624a6b75546e54480a366c3863446c2f586e764
661535a5148464c516a6f793507 64c426b3135706f5466526266306a2b6c
437053703135396467346952 2b756a625376344b6a48520a33733979394f5
63141674d4241414543676745416156413436 4c554771742b694f50503572
784d65546c654d392b4e5166762b2f415a77564569736f596d52370a63446
930525a676a2f78564f486361304d565a70446667496544354a796a482b31
7831646e4a4f472f57446e344a6b6c6f57446c7937346e46314a7738664e4
b0a464d4431547456626736 4b5473302f426a68744c5a6b69756c63636e78
7a774a35786857334c6d466a6c716263766f32587976447a79527858727a3
8444f4c6c0a4b7a6c6a4d7169624d6f7953574d2b2f497a4d6f734c517a33
6c30674367424c49334e587559324c736e6f4b38426a314a484a3569674c3
278622f456a4a796b0a59742f4b676b4b5167574e4a596252564646467035
494139656c63515131667a66776a2f417276734a3858414c464943326c657
343705a594d47776276455a410a54706774422f61576361534e484443732b
4b724d6c716b6a6c35622b625847303445315154453746 41514b426751443
95773783233416e6e5531364f6f5a646a0a4d684137495361356b6434684d
4d704c38454d4c4a74556947594c7474716369554953 4d48497a4f6563427
a734e6f4a39447144474233766c6a4d6e514e73450a7266536c75426e3472
747161594538696b3459376b55474e7771552b4e4f726a676e66586a67694
5624e712b4f363146474f304942376c594c41766e303736740a692f796e58
6254422b545a342b696e3778495952754e314151514b42675144346b4a397
6726b5273756153474e5879497256706e484533466b444641346a4d410a38
4773354f7248782f48556a6d5547424863354f6e6568717975474b6841525
1556d64534c72574e3863785236504f684d576a76775730694c4d51457255
2f740a4c6b4f6e37636f2f6f39584c3165784f556273666c7a7666484c625
375574a484c593943656a6e32484d5235494175316265556 84a3436384e41
37594778516c0a45416c64447743594e514b426744785a63356a676779397
14b587a364f76427a445843345464776f5265784d44665157304447493133
3465363551715452656 30a62475a667170374957374a7a4c777a74387a346
b385953506c3748432f696a594d7732436c4255727559444b626939445374
64486d34446b47363538746e4c700a4d686a546957335a37435569572f793
46d6b57756156543663502b513762757a4f385332536f646d454c61796947
756a665867644f2f3742416f4741546c54640a4f636530586f4d655777454
f447442366c6458776d4672356570594f4e72534e5263712b657944784656
666473622f66335279634f744e57776c30614d756e560a443677536f506e6
25274446676694f68437a56736e4146356748505270564159474271797974
3170716350767054725365 6f4568614131586641375a3773356e0a7743356
568375848494e6939643935362f376a456e594457554c6f76336749777754
665347795543675942 2b6b77575a474e59707577584e76486a42646a4a6e0
a62455a2f665952712f735278772b52556347546b665438566e355850614c
457032726149642b52674c6c65777345704f77447753624a7868626a31505
1324f490a62744f716e476d31362b41434d556f7457343477524c72395469
4844793059444a7154734577326a4d34596c726b63386e6e77335748596a4
e2b74474d7a646d0a6872444337724150475 76a4638343964547677654677
```

```
      3d3d0a2d2d2d2d2d454e442050524956415445204b45592d2d2d2d2d0a
      pkS: 30820152303d06092a864886f70d01010a3030a00d300b0609608648
      016503040202a11a301806092a864886f70d010108300b060960864801650
      3040202a2030201300382010f003082010a0282010100f5ff16f013d9468f
      924b83ada75fc0f23f97077505bdf5ed45666d20f32acc439c0118a185519
      39404514ea6513030dae072f3a39d4b374389cbc198b66c4d206f954bce04
      ee917cffd82bc605215a52cb456afb975065b0a7f427d99390d665dc11bed
      b586b5c204f7243fe6761b23de1e35890fa9a179609f2a0e3df81a9fe17a9
      8c9b178c4eea4f6eb56da62bfd7f489f491d03a97db81f0b46fb5968d5704
      e60c486769b673a93025429f2fdf20445eca1c126226e7774270b70620c6c
      ff2916db986c992e4e74c7ea5f1c0e5fd79ef15a49940714b423a32dcfbcb
      064d79a684df45b7f48fe942a52a75e7d760e2247eba36d2bf82a31d1decf
      72f4e5750203010001
      token_challenge: 0002000b497373756572204e616d652011510a693c9a
      5af2115e1d93646ec55d3696ce6627d8f595be05f0db23a7d5e40005612c6
      22c63
      nonce: af2dc5bf9e3a6d3b4a625bac32e19061774901c937d97f9a48df38
      1cd372c3a7
      blind: de888a141ab0adf0ff07e4cc929b6ac1a599e65c3ee6f4e2c602b0
      fcb47a08712c7f2ef6f3fc0fffd6572c66498cf044aaceac28c56dfba5faf
      36b5c74bb40aa76aba559f44203816512bcedee9d168e2bcca80c889fd74a
      f02fe24c22eee7014443bbf4d304e47c9686db966aebbb5543a07b37036ed
      03d844202de9c3ee59c8a1ebea14c1e572f2aaed214f831e1faa269854ccf
      f13e62f0f144dffc9b2e982b7632d8977f815f294aed7a5f544b038f7fbbe
      33fec777586174ceda91c7579da859563da8272fbd48dcb665c4342fb1724
      9bf87846534cd60e224cec187f02e14b91bb68bce3a4b7c135286f104916d
      d2cf9dcea44797fd7057073a0cc69bd
      token: 0002af2dc5bf9e3a6d3b4a625bac32e19061774901c937d97f9a48
      df381cd372c3a726667f6916c5aea78f184c27002c95dd4ed283189a68224
      ad7f322ef706a3b58c19b7457b57865de3c54bd8b1860fed5ab4c868bbb32
      4145f17f74e77c77be9538216d8140ca0c87bf4cd17077f1a82e6aedd2255
      051191f5006f10b06ec8db240ebfc98fd80a9c1bea8f3c00d38902c2cde35
      7c40f098f0705605002afb9e80eea058602e5fc86b272b9bdac0d68c80347
      51dee5ef2c7e4ed5424e66b52ad16ba78b1153410ce94207b91646079b25d
      f936c577d747aec615797bd9e96ba8dea30c7c3dbe4aa0f1b687fb865c36f
      197cb19df9f7c2457874185b869cd7428af0227baa64fe98e09ceb4a4f76b
      ba48f67064161bd13c5390658eb0a1a135de3b27c408402aaf280d54a438d
      51756ec2585b5da29fcb1c8a005a747414874276c92996ec414a8ac4eff1c
      57cfea3b9010781d9aec15a32f1307f557581c6bf507
   token_request: 4137000173039e6793ea9ad36c05b19247a450f78c9a6598f0
   69579102c98723c534779461e54b5220d83d2c4f975a40d0a77de8498c000295a
   16b1f1b469884a38ef1c7e691ad0355ee59bb4ad462934dc15dac6294a57030fe
   83677e31c806c07ed9ca3450a26de0607c4596509a5c6128ff1e788f9b0fae40a
   130a0e022e5026fc34c44d6223525dfe181a603bed2ee58a91718e4550e65396d
   721768605adb7b82765ffd1769f1a3d2d5d62160025bc7c16803d0af81f969359
   160e11cc1862dcc2ad643a055daf7c94f9a5a351dce3e2f1da19b1d3270fa6b72
   d3f568952978404454a9022fa1d078478073a7615ffa6ebeda95621c140759867
   15e0b25ecee559b0e78e0074b297632f536faca4fba86e6f7d6062520dfa47283
```

```
   996ff2a297be0eea01cf4c37b575f64d9a65a5140f40d37a8223bc4c
   token_response: 419701000102960715043dcddc055f5805a41e2fc119ee58c
   d8d0fd057fb9dd9d6b6adc97f5d3b6c46fe36cf6fdcbc73c6aa049a04bdc6d824
   fc505b2683b9d1b023324fb3a87282fbb7d8ac5f95611426bb1e9d37909b6304e
   19743c4c5276aa6c8182bc9f5b7ab71f31aa75bd0aa587f16ca093ab1ba1f7a17
   0e1d16df59a598bb64e6a97fd8cca72a87ed8b2eaea501c7a1ef5ac001000297c
   fa38a3fab7aff07a6f1ad9c022692309c76aa657149afdac4cc4dce735b415ea3
   0c9ba4b04f3320542e2c4f5af190af826ae264b6cf3abdd0a559cf8868ed5490f
   f9d21e04a8ae12eaa95adf28293e1b27425e02e2539caebf5849b281b2475084b
   daa2bf368d7cb0e6126092540aa5511db0f507249be6af93e4c2745db6d6689ea
   c80e499e2c54e392e17be76a4c3441e66bb5ba608a5b32f102ad434c691e82828
   946d1dd3587f68acde191f4d7933f3f5649ef5255e4f8b6a1fddc85974603e5c5
   ff87a9f6209f1aeb7b01919e751da5de3341ba8044f5419fb2fb6125b08a27ac0
   185a976d82ecb5fd6cc0508f96ff8290939e869641907cc8b60186

   // Test vector 7:
   issuance:
     - type: 0002
       skS: 2d2d2d2d2d424547494e20505249564154452044b45592d2d2d2d2d0a
       4d4949457667494241444414e42676b71686b69473977302415145464141 5
       343424b67776767536b41674541416f4942415143794231723031627043 72
       7969360a4238596c68415a544c51306c762f79416d4d4b346d69744458457
       44f654a7a6d4244556630324c696d775573477472637a6270367541466551
       796e49504134300a3642774859482b3254674f375745426b694b563776456
       e71673471727a7356785a7572337255496850475a717a654b477970357476
       51617741624b65436654590a5546485850346758696f587a556e39634a716
       94e707756343245475133584738736f716d4b777a5273665a7256474f7a46
       31734a55425964332f71365a327a660a6f5a64514f34325343544d5878623
       46558344e536771535935593747494357767457364e6c71412b7132596b78
       4a2b3855534f743941703477474a73355030360a717677564a4a737857437
       8556e6f6a665478456439487959485 54a4d614e416c58344b6a79626b6151
       3250496865765a4a473035694d4549627457694875596e0a3534577a376f4
       d4441674d424141454367674542414c42356c424e686a6971755156767665
       7438546563575877684771743532755545 2f3447327a426e3744670a35503
       8714b704d71307a6f3457793832533842586530524e424b597851386a4770
       3371516e384138537a306e4a704865304b34587570726d7367727a6246495
       60a50536e46304b50474c75694e5843554268453044713371797831395076
       34546a37373943463236632f73582f5066744f7977744a4577716742302b6
       35a356f320a454e48395a5176634d4e653869322b376a4577526246365430
       6e6e4f752b7351433435474956616 34b594c41705a4c74305253343336486
       6463141555052496 60a2b4c794a32385855534749495 3496b716e75367379
       7866444551534534556a7a355371674135646d58654c6f5076624369454a3
       270742b466d504b5649626c370a32776754592b496d37784b314551396432
       735a4666544f6a7437646e596954736f47626c376151657a3545436759454
       136484a434966306b2b43616b454c74330a4a724364334a4164787a674d2b
       7637764569624c4441542f5562792b674f6f454b3835613244624a4f6f474
       b66673276342f525837694c4e414c453635774d540a4774675077704e6854
       31654451444c56486e7a715a6245495a703361745239386e596f4876634f7
```

```
875716b36473379516d427754557662304e306936482f2f410a7661354363
744745384e536c7858313869494c5676754f7735697343675945417842463
84b4e566e316746634172356c71306a5372766864773858686696e45500a62
4134754e6a692b665435467362496159474561307978587685a316735413
6687764726932326f2b59544b696d64697a7a764733685045 5a4232534464
572b0a384272325476393076635133417a466341654352463479797956633
67a674d7147797235346952625 22f6a65322b36793353775a625a7a5a7667
4956476a4c420a4674696863377a6c416f6b436759417934413870635561 4
f4b61627649706a4a6c773532482f546b6a5a674a74354b4c336f48436437
574b4a6b3172326378660a36694a6f4146573677472b586431647742534c5
a74445136577041527a394a3270614f4e617352356f5358512f3038324252
456f674c3764397437506c62796f0a6e6e566a53316d7a435362327253545
970677830744368766b544e726e59614a2f594839723233786142 6d415342
37686f674532626f396855514b42674668700a53674e6674364c596d68546
9706858476b4c6f315a4a4b532b46446c436e382f4a626474667667617a48
4b4554554349695141515473 4a47506c6446416839420a5355316c3958774
f56515a7a2b43706157694a70353354396f49353867387a6857342f6a7756
43513266326d6c456145624f69686d54305243494d3943672b570a4958664
87a5346334a34636b36364b7638416474597749374469 6a7947662b6a5436
7051307a4f42416f4742414f474a70612b783237382f68527a5948414e6c0
a5542426e4c7556794537437974334396d632f6a36564a7766765a2f617331
4e5133664a615551546330334b6347467363354c6338567a73567a336e694
36a324d0a6431574356354c6a6c377763302f6743423863794774316555577
4f713258556d4c6d73365a53434f694b6c674a662f364178635a65764f316
543344c46726e4b0a397a597955646e476a716d59436d4d33347566434556
70370a2d2d2d2d2d454e4420505249564154 45204b45592d2d2d2d2d0a
pkS: 30820152303d06092a864886f70d01010a3030a00d300b0609608648
016503040202a11a301806092a864886f70d010108300b060960864801650
3040202a203020130038201 0f003082010a0282010100b2075af4d5ba42af
28ba07c6258406532d0d25bffc8098c2b89a2b435c4b4e789ce604351fd36
2e29b052c1adadccdba7ab8015e4329c83c0e34e81c07607fb64e03bb5840
6488a57bbc49ea838aabcec57166eaf7ad42213c666acde286ca9e6dbd06b
001b29e09f4d85051d73f88178a85f3527f5c26a88da70578d84190dd71bc
b28aa62b0cd1b1f66b5463b3175b0950161ddffaba676cdfa197503b8d920
93317c5be1e5f835282a498e58ec62025afb56e8d96a03eab6624c49fbc51
23adf40a78c0626ce4fd3aaafc15249b31582c549e88df4f111df47c981d4
24c68d0255f82a3c9b91a4363c885ebd9246d3988c1086ed5a21ee627e785
b3ee83030203010001
token_challenge:
0002000b497373756572204e616d65000005612c622c63
nonce: d0e02f3aab17957e678918b88bd107d001146822edecfa9286827f
8cd2e887d0
blind: 8fbb53b0b61268491d30a0b56b8184746e211031462a112a4259cc
29c948bbf9ea2bc5c1b395185e2f9f422235d55f37f4334f080d947a66e47
e9e842b4e663cbf7b5d2e648c8e987db8b3ffba9ef991b7e4b25d1c2e3b17
26226244690237d4c1599d50efac6571f7173a67f4c93d07ca5b91ceb3188
4ede2475f3fcd52eb72cb38ddf18e37563b8d4b1f1397f05df3e6d65bdc7f
909f4302088984637742 30ab47124a987c776e8224ae9b835889e88ab306f
```

```
      1ef397e0538ab93f681e563a83432b120f4dcd336bfea0978fd6d1aa06dfe
      635a0a1c1729ced586054d304af479c408e564d50473d86d0c84a1c55ac1e
      efda6347898722e5b60e02d56a495dd
      token: 0002d0e02f3aab17957e678918b88bd107d001146822edecfa9286
      827f8cd2e887d0201c8af95ce37c05aaa2acadc50fd6d8a825e992c5bebf2
      d617f0359cbb669d85847ee9ca05f3abc8de756db4181bb525ab806888d71
      f3313c37d63d50b05e2aa479db91b2e7175b49cc8c580bdf48541c252ee23
      754b999ccd309e3d51740be0da7f346689617a8421d47d5803b1b9e38dadb
      f6dd377f8553d86d5362124d154457f4318ecf67346cd553c684b3c4e56b2
      0083e195c0f944c7fbd941dba0e0946d03d9750ce0be2470a9f3abc68185c
      93bc2e6dc2bcf84d61a50f96e9b229ef7308aac70b86e61c5bbfcff34eb2c
      23cfaab41c8775c38d6f095d56d4e43f3af8c8919dd6d11964038aac6245c
      7c7914a3e6c171cf262d67cf021f6c37621a6ca4f300d9141141ce8bc484d
      fbdc8d57572554b4424021014f7a07f5eeb9ef8c9827abd018f257cf1ac74
      9e5d35dfcadab80abb9e2aaeaa76d4f1c2dfdd5ff7f5
    - type: 0001
      skS: 79d090708ee7b744f1a764a345cf5ed372b0d12dbb02b8ede06dd649
      712e1091af235466040b350d5fd547ab3b23aad7
      pkS: 02e26e2214b4307c84c9bcce7cf89d90a65ac201d5c6972f59e66afd
      3e4a543addfadd364bf8d5a503f66e3bfbc358138b
      token_challenge: 0001000b497373756572204e616d6520f367e2f0d174
      4a7ebb63ec0e7d80be9d32314ed9c4d163894debca99cd02fcc30005612c6
      22c63
      nonce: 4e39a695d77cb30da3dd7853fab3d8ad903aed8507559a158df4b0
      5510dd6db7
      blind: 1b48f7d21eae4826dc45097a7265186cc3d5c809889fed2ae498db
      a33c34a630106f9551ae7ccd0471a1d89ed7c7c243
      token: 00014e39a695d77cb30da3dd7853fab3d8ad903aed8507559a158d
      f4b05510dd6db7a4daeb7e44acdc36c1556bb646f452343e6f33bf6c61340
      efe89e94d0026f245cc5ac4950d730cea0a8fef3f63d769d002fd4655e786
      156b2ea5a99e26aa0694a1b0b9bbff925e2fc7cc82fdbff60bddc4b4e0b07
      76d2a0f4085c7c914eb310891b1bda47deb869861c4f23de498a6ef
  token_request: 413700022a1b4a45b6c832014f518cbf671f5069a9bffa7c98
  ed82d9df888a470cb60ef6f8951433a9d515304513313996bb5693f23d9be93e5
  6ac59df72d7644604e316c6e779d178e91de907935b762f08a2516fcd2b32c5ec
  305bd96a44e420660d9fa6d1ed89050fcc538ca3a4afba2e1cb49c611b7491803
  8c2231a4a0e85f7173260f31cd1ed6a0f3a3ec5c40d58833fb09e55c6191b7c0a
  3ed061dcc7d78ce972f7184bb8181010a650b36bba472938c8190b9cc2bc3df84
  36a425723d6230aa91d397ffd680e6ab12ea7586ca168c43790ece3d9eaac1a03
  a98132b70008eb6a9afcdb41a15a21fc59f5efff31e17b26c6c884a3f21f26ec8
  e46813753439fbb0a000194034f03b6b499800ef6c4ff5ae4e3ba6c71c8757e65
  c1f2533e84fbf1c04dc102100ee8717427f6833347f467311ea53acb
  token_response: 4197010002198be0563250be6ba529e2b1acc30a3c4564019
  c227856609344adbd574be40d0b5ee9f0ba071711e6f10075ed83a3c530342ebc
  c7fd54a4421b93fd98e9cd61c27128bbceff0d1eeffd2e59523c7f101864ca97e
  2f889189263feb351499c0319a5a612d74a2650772c58e109ff7db789a9f10ef1
  ca409fa4541658b6e70128cc9ed23d0390b5ea529aeb4f017f099b6f0768a10a0
  d021abe578b85a289d22928ab51b4c07da71016a6a2e49c800a4dc0bc767ec2b0
```

```
   2a1eba7baa94efcd582215a07201f5b1b9c5cade04bbeed6e82abf8235003bfb1
   6f8d346112c3f865a4d6398571a5e6da96d6d810a6016433c258bb261c6da3824
   142f1b283a62038db901000102cd0c4e0dda07218612009f7402d1d4230449ef4
   5e01a9d5a11424d49e3828d47331ad9a24ea960b3653e8a00f0b4ffaadc12d787
   feba11edfbb1dc171fe391f8a3c1980125f5c909fb3e1bdcc34b65d3b68261c0c
   d5e0fd521035173e0c6043701697c03cd73fab74694f53aaed84791a58ec78add
   1c7b754b4a5d25a7dfab21b27942dcfc732a4457dbdcede8a89886

   // Test vector 8:
   issuance:
     - type: 0001
       skS: d02a980087c445cda954f20f236f0412682179ef1febd1389e9ff64f
       4da210386dc01a8ff3c6e1ec36a9332ed45fc4f0
       pkS: 0354923576bafce71b63ad46ea61ee24a0815030bc9b6434817fd0a9
       b7946d98670e4556eb26793e7c0e8bc49712746b9f
       token_challenge:
       0001000b497373756572204e616d65000005612c622c63
       nonce: 359ebf6bbc1380f49232d5308c9503c64acc81eae1fc9e6c22990c
       730439ff58
       blind: dc34ce1a57daccd8d8e41a5003baf3bbdb3c6a03b0c29362a13751
       5d3e0105622b31cdb8da507772ae7169bbd0be73fb
       token: 0001359ebf6bbc1380f49232d5308c9503c64acc81eae1fc9e6c22
       990c730439ff584d1a8f1a708ab7ec6f9ddfe97074859fdf87737790491e4
       b3afd0977cd3bd39698b261adecfad413af272471a45f97a1bb710bf4ad9e
       9ceab9dd4257021a50c27eec8338c740dac91522f5cbeb66655e000a77504
       c986d077fcac0b4908883d7ca92fe82779c4f68c5379e4f250e38b1
     - type: 0002
       skS: 2d2d2d2d2d424547494e20505249564154204b45592d2d2d2d2d0a
       4d4949457651494241444414e42676b71686b6947397730424151454641415
       343424b63776767536a41674541416f4942415143625170507641456732 4a
       6a45790a614d6a477042516b5035677556747a764c582f4a6664413652777
       662496b3850505735453377316461412f4c7a6563316651356f4e58314966
       336879316447670a74307141473156582b34566b4550672b5334554d424e5
       a4342586d4635544b52654c386456644258454a75684f48357044666b516b
       7370454a455a344a656e740a6d7574683544554f5075504d706c39674f2b4
       b3745783936645162444c7731766748486563457739324235703870716462
       7a4838654d6256577235597a362b530a316a4242415362785974457030413
       3702b79706d6854596338786847502f3551414f61444e462b746e59543638
       306e76787832566e50784a3758716b316e49490a4d64647a4f582f54684f6
       74e2f584a4c37416c3462676d326d6d475a466f79614e69323378666d7654
       443654664d683873507377416e6a457746724b7366484d0a4b626a6d43786
       63541674d4241414543676745424 14a66344c76793964664571715055436 7
       364f4c627675634538556e324e467a3436544274564f56767845620a482b3
       9323362776a3539304a776f786d576d324d6e744635716375516d63457463
       536179776756717537714777795954526 96b546d6f4d4e4b507375694b683
       60a6b3269346d376948436f70754179646e4f4c527a724e7141452b4e6d37
       6d4d6b47546b74626b412f4d3339694a32396c576533454d4557556a6a633
       63351656d0a504646592b6950635657554e7150656d7149664a757972394a
```

```
5258356d4e6c33396f55413773342b795656325a4c59706a58583746475a4
479416643754368420a6e525848642f525137566a45307235786550337a73
346d4f5550646e4e776b446d716c4569726c7032454d54652b7a2f4d74364
94e456258744e543779506f4e0a5a3168742f78635173714a634358445075
56525775684e734e48524b4661372b39357557765236674a3045436759454
17979736352316b4d4c2b5a45474f466d0a6d62455138684c493870427379
666137495434413 82f69384f4e2b78337430654378656c324c4954384e415
948664763657736667a59426432517968634f64470a6f6f7a774978795735
506237553839764a70504d73784453695a58746a5a782f52745a2b4271785
16f702f6567682f676c52576c6b3444474c75733246744e730a734a2f4658
5a576941744770674c2f5033703965792f58334b345543675945417736493
36c552b4e764d67533533516c786e6b4368366e2b4c50724a5272464a0a4c
374c484a413235374e4b766e4f55562f5553777a324235315737494c48567
a706d695647546775332f7643456731756c33554e42674a516e4e6b747735
73730a38334a61344c3278572f4150505850547331526674 6e63314437417
24b4f563268426a76746c365770774d746a7459696d684c58374775515863
2b346a4d62670a7453683950772f376f75554367594234434d42735a76414
d584c396538387a7167504c434574636d654b334e705468714b33666b724e
43487961494e536861310a39774c46524845446c653670776c5878586e4b4
c74347536385074772b544f43566b4b4b66426d71725546514176356f6a47
6f6b5959774350644a6347466f610a51422b31555a6c53653647367635717
7656c6d5a4444774b2f4779346a37466e715032796a5056724e5051775853
4d7a4a4857646933533941514b42674867510a4c57617754542b4831726f2
f75524e476e7676646f3057396f4275486f472f716d336351435952446855
32583974665a2b56303853326c6d744f6b384a2f372f0a2f6b6c6442722b6
d426551495a4641466f546d4834437479796a68624773704a363259305a51
34556c5858556952397337395 44f386a79766c4c316a6e6b6e520a2b41514
870785057796e583443344a646744447a6a7356555032482b69466747416c
2f616b6b6656416f4741413064693773337030 7a556943663869786b53540
a6a61686c5a5a6d535670795a76654b6f5434334546564277687746557 36e
3232436a68717141596856595344 4d724c624e39695764674c79645839304
d3461580a2b41663976505463532b686553355a3172584432564f6b682b33
616a4c542b537479726679446d5a52637332694e624e43416746666c70663
863363447394a690a5656715761384461694769 76c2f49746167337a374d7661
413d0a2d2d2d2d2d454e44205052495641544520 4b45592d2d2d2d2d0a
pkS: 30820152303d06092a864886f70d01010a3030a00d300b0609608648
016503040202a11a301806092a864886f70d010108300b060960864801650
3040202a203020130038201 0f003082010a02820101009b4293ef00483626
313268c8c6a414243f982e56dcef2d7fc97dd03a470bdb224f0f3d6e44df0
d5d680fcbcde7357d0e68357d487f7872d5d1a0b74a801b5557fb856410f8
3e4b850c04d642057985e5329178bf1d55d057109ba1387e690df91092ca4
424467825e9ed9aeb61e4350e3ee3cca65f603be2bb131f7a7506c32f0d6f
8071de704c3dd81e69f29a9d6f31fc78c6d55abe58cfaf92d630410126f16
2d129d00de9fb2a6685361cf318463ffe5000e683345fad9d84faf349efc7
1d959cfc49ed7aa4d6720831d773397fd384e80dfd724bec09786e09b69a6
199168c9a362db7c5f9af4c3e937cc87cb0fb300278c4c05acab1f1cc29b8
e60b17f90203010001
token_challenge:
```

```
      0002000b497373756572204e616d65000005612c622c63
      nonce: e2ae9b0649b5aba135b7be7c357c2928f66bfb1134c0ffb4b28adc
      64d6e11c5d
      blind: 39d78a7e2fc369e1055f4db77ffeecc3e364b33a37690f4984b39d
      01063537351619bad1103a5875d1a2f1dd41c1dc1a11999b90d9c58127ee7
      f579ec9b7d30ef71f87b4ee708bdb3d279cb063a3f9893712162f47d9cc3d
      00b3a1b7ceba6071dff7409c330f4d0421486cec20b0df5f7c8e689c00caf
      9c7060bee6e15560d4e942b670013a8ab1f13ab82cdbdfd248959d404b284
      53bb7a2792a468e7682c4df7d999008930e0d2fc9e5c460924c3850db854c
      ab5e838e49c8f69903c1c0eec89949fe535035a3ad343435fdc6f2a04a2f0
      3558e7fe89e4d74f883ea45adf5247f9e9f8b96708e45cf94c9db46ad641d
      1c73b09f6d40a85ea1d3f61e4992a36
      token: 0002e2ae9b0649b5aba135b7be7c357c2928f66bfb1134c0ffb4b2
      8adc64d6e11c5d201c8af95ce37c05aaa2acadc50fd6d8a825e992c5bebf2
      d617f0359cbb669d8edaf9c963ed48825384a11a159d9ef41b054e62eb0e6
      139e255ead44f73f95eb799d1138d55a16d87aa75fa0504bc82623c342204
      ca15084fa9356af319b4520b06241d549c8a0fcff311c3d609f29a90ff912
      1756bf73421083d93cde93971cb38da8e0379d22642580d03500ad1439db9
      35ef7bf1449ab5a05d74db678ba4432df8bc3ea1fba0e8e25bc54a6282450
      03d88117ac961ccb614cd17aa795801ab3f918b67e2d863aa9d833800e546
      91b274cf4c3699f59ec0fa79b00dac7379c341fc86c8cf19609168a8b5bc9
      224bf76469dd88c62e00048236c8c8da2d73110bafb17e764e971a3f8f335
      0f461103f131dd915f003a34445385069481ce90b5e52080c4e14a29c9849
      d3bc45968184f5478bd1baca0f4068004b724f3f8717
    - type: 0005
      skS: 0f69c96fbee5d5bf753ea38c5a389d8442789bce712c379c0df7c9e9
      71ed340f
      pkS: 7061a3a2e6e145f1271f5d23c10fdf33f3dd0a02bb13b21ba607f491
      35bdb20b
      token_challenge: 0005000b497373756572204e616d6520e41785c1b1b2
      14e373a34a43b761d67f4c712eea2a2ef52d9fdfa93e74ae79a80005612c6
      22c63
      nonce: 15af88cd527637b15c1ddcc7bd5f82d4aaecbc5f18d4c21e45d6f7
      53b658762d
      blind: 9d74573b31139fcfdf49f5b082b8877fa9e016897117647438325e
      4ee09ddb03
      token: 000515af88cd527637b15c1ddcc7bd5f82d4aaecbc5f18d4c21e45
      d6f753b658762d136301b885d88ccc995b0b3be353349282cbfe97be12b38
      740d4bcae9d1d15f65ccde68c832ff8cf4c532d76e07a2063b1badcb020fe
      a2bd12657da4075b228502a095ce39773e135c62765fc6141d88548a7a036
      0b111e655d6830486cf213d73549eceafee1be703beec3e9fa8059ed370cd
      ec0efa2472f4298ca345e1badd
    - type: 0002
      skS: 2d2d2d2d2d424547494e20505249564154455204b45592d2d2d2d2d0a
      4d4949457667494241444414e42676b71686b6947397730424151454641415
      343424b67776767536b41674541416f49424151445a36557646474a4a6b66
      76336e0a4c6478574964557073 4c36596b7442495359784844644e6151574
      3615455722f6d6b5649455753626a46576a6a362f59335837544d4c545279
```

```
48737466444c530a6879384e6f7477764b34355076652b584c2b79736f796
d597776574f312b6b7965316e553061543166424a474b504f494954704768
6e6e566336553961585 14e0a665333676a655739767a3369574a666961774
84c6b326f6c6c376362786467755 96d416e535578337958322f596f526f4b
644e54647576642f46663553684a750a444250397671426b4c42334545694
24f47567a59454f4248464e2f5a6c646e7930737a365956705a777379506d
4554424a54356b426a3575746242725879745 10a4d4a45786c302b6c69573
375794c63495952657344387a6f4f616b47617a2f594d6e563171714d364a
5631526669305 2366b6c4432696b646a624271436550670a63784d3073593
15441674d4241414543676745424 14b754654346566464c4f587063444f76
307a6f716f4637526a71503750504a4f477042507167664a3675730a78536
931784779366a4164486961304a6a323953774e3334793473496b37513075
30677338654e34326e6b69666f7a5477762b7330457a2b7a4f49614b76433
50a6b4375564868732b764f6f684d373058784d44553771724f644a324876
6e7539516f54506b456e64527756347633776e49623474586964674c442f5
530474e420a666c71326a746f6335677539467637694 7b33534c692b38
64326c4a2f4b4243596f4547755046514643526a2b735876684a744c70797
166644e54386e397a0a4545534566364e74384a684779426f3466444a4139
4f4e416c6c61644875474c6b6a30465557786c6e7a66656d733133686a335
56a31584157506f65504d58660a6131796a6e466e386934485742446f7847
4952776759477668657a3333323732516368314450 2f386e4e6b436759454
137495055704b4a454735487538674e720a354b7458507931684254785467
4b7556366572646a47377447644b6c46392b713579744b45646572696a456
a644c6e34387638484f3166566a394131374163430a6a476f7a37706f5268
766252364d6752306b4848417849456555627 82b61775a72714f5256416d4
2423339456f7441596f4136586f764774573465306e3362470a4e47365449
6a7672784f4e6d784f7738376635466666596a3150634367594541363930 6
2347342534537716779424958477 36e49632b47614b49687872454f4d0a31
2f704e68466a2f576351706a47684e6c784763337a5a377a6774703061665
06d6a4a5466766e4234365738695778747 56f7966696e5470764831546d30
49650a34694d326a37652f777646774d33464a596a4f6a4b4b5962697a2f2
f775136426c627056735450397a774831743257615354853374173 6f4a4f
6b7177516c570a67656c34464a794748345543675941367569314678 2b6a6
a6336514351656b376558514c67756752566235694e376a637757334c6e67
75506d756456657a74440a64564e4b424f526152774e4879356e4f4e4a634
7484451794a6f414e494678346f7a4a4c37384f6b594973556f7745523154
566d524d594a6d783067597152700a3463474850576a6c684b74315266696
e585a67335a49306f4b68556d6432615678464d536342434637665570746f
4d576b556d4f456c307056774b4267485a470a6970564b6d3934493246643
775747055465a4547734b6469784a333977634d4d595a4c636a6a41566a6b
41366a6134547876616e2b36313353376b327a59516c0a65486c554255614
33965687a31784b564d657663644e6c7766317837363843367038477141 78
396573305559716850306b507a785478366c475474576175554b0a6136355
178425871686131523565794f62356175675a4d4132632b7a5077346d5a58
44776a4e4742416f4742414b5a5a4135747a597638636373325157637251 0
a4763374641747a444979675a3336674f4964366535494c7234516d357447
704d72784669685742485279665 07a6c6d702f4d57483839632f59384a4e5
9534e480a774e63526c306c45527170544b6e664d316a3234484477696677
```

```
      4f53412b744c7a586475704f546f2f736634705062587756475733794178 3
      6697973533878500a77307a544b65497165434f79684942324c4242583872
      79660a2d2d2d2d2d454e442050524956415445204b45592d2d2d2d2d0a
      pkS: 30820152303d06092a864886f70d01010a3030a00d300b0609608648
      016503040202a11a301806092a864886f70d010108300b060960864801650
      3040202a203020130038201 0f003082010a0282010100d9e94bc51892647e
      fde72ddc5621d529b0be9892d048498c470dd35a41609a4d4aff9a4548116
      49b8c55a38fafd8dd7ed330b4d1c87b2d7c32d2872f0da2dc2f2b8e4fbdef
      972fecaca32998c2f58ed7e9327b59d4d1a4f57c124628f388213a468679d
      573a53d69740d7d2de08de5bdbf3de25897e26b01cb936a2597b71bc5d82e
      626027494c77c97dbf62846829d35376ebddfc57f94a126e0c13fdbea0642
      c1dc412204e195cd810e04714dfd995d9f2d2ccfa615a59c2cc8f9844c125
      3e64063e6eb5b06b5f2b50309131974fa5896deec8b7086117ac0fcce839a
      9066b3fd8327575aaa33a255d517e2d11ea4943da291d8db06a09e3e07313
      34b18d530203010001
      token_challenge: 0002000b497373756572204e616d6520fee606b45d79
      071ebc3d4b1578e9fba6d0203b37b634396c9319bc84fd337bfc0005612c6
      22c63
      nonce: 091cb6b53c06d676e883a5e849175b7ada9447e9ffa1340bdbf903
      bbe8dfeeee
      blind: 38ab5daff76b99756c5139fe9f05c681db94cf94d4a99cd0266a56
      3963844dee65be736e16d123c1966390d31952813df3a70986446168e9737
      bede3e3230f234e67233aaec48ca34614243e8dfdabcd5de050fa41bbcf40
      63f9e17abe555610fab025f5328a50c40f466831dcb7c39677c9212ac7a95
      31f31bf4a976d9e3960d36c7e268530c36b80e34eab97c0f7aa3dafebc692
      767b25746c0764670651720e363e2c24404a8bfc0055baa48ee0fb456f91d
      e5afaa90ba90c0465b6ab6e29b98c1cb0aa7608008ef38c5774f576dc5ece
      a6f4e44220835f6405c50110eb4746a3e3ff9b39cffdc2196202802a72df2
      aa7608139b364b3d87540b3a9291050
      token: 0002091cb6b53c06d676e883a5e849175b7ada9447e9ffa1340bdb
      f903bbe8dfeeeefef1a842ffd4750abf64ceb2f6acd5662c25a58c314f6da
      f6fb1b3eb46506119ae9b682e9726d3674ef03bae444bc47bd2ab94c9f906
      6144c4fcc4bcc30ba00534c8705e3329cb5ae5886669a137bf3f14d322b62
      1065f3f1c3afdfc1358db4728cff35a3c7f4c98bf6c9b36365846692b3274
      b1bddabc7aa4ef1fccf91bf940c01da83c3d2e14441b8c1133c7da74e28cb
      197db5334d9218f418d159683eb70caf998f2267527cc331086af60baa390
      f83384a39257ec56e68f8b008404f99c40e11d696115312e316314b9c5c68
      0d0768354ecf433cd95283206600bcd669fb9bc2bd2541e8c8a7aa6b764c1
      16183448d034d0ac1fcab5f28b86ef0c7c0d0cf2e58ed472805d4af0faeb9
      7df388f7f63fd25b6711d39666ca52d03cb078692fe5c6fcf9f1aa0791c18
      16412c9da990e74f5075255e6e1917edf2a06b4c4a67
   token_request: 425d0001c202b2634407d8ff619b802022b08f412569998697
   d1dfa28eb27a43c8558234d590c249c13d4333d4a5c56e8bba47380c6d0002eb3
   6f3b947adad194dd8a857d7afaaec606cfe2ea9b094cb4498556ccc9c941d31c8
   154574cf7867231916864214cf008c858296d427a1b53e3fd0a383ad35ee09437
   ec019b3cb6153cb812034a2ddb1d9687cf65d8a62d370a144b99bcbfbcd71775b
   0572318c5aed0b59d99fd53c48d04c44700791a154483d57c8acaaafdc1111ee6
   173a8c8feb353d1c10b81136701e2e018df16e09b2a07e4332dda3e1f9dd843d8
```

```
   e48409e141d71d711cac3b813d74ad28acb1b2db90317826af754c9d6679d66ae
   f57cc7a7950588f9c579b6802af1147da8820017bd13ccc02b7aeb712a13aeb53
   8685864de542e7002bb6428ccb216c07546b3ded3cd9d84a37ff2dea0005851c8
   2537d5b9c89fdf936772461fc3fd14ff36981b5eea1b26a5d19311091b40e0002
   05236dd0c66157e07afe8f74407816aa87b0fc8a773538e73c7673f80b900bc3a
   5b0570b7feb7c5aafb5b0006601c43cb87c96dbac850826e9e4b612f81fe7bae0
   67220b057c1464c44bb4c1306e554a28efde7b536ffab073658a3a64ad963394b
   fdd565bdec31d52dd3e8294f7580fc97ba30e72c6bd58089d9a3d59e531789104
   38bd576c94504458206e6612d4c8e38eb553776b99cc3cfd8f46583280055c6a2
   2445f7a5bec1d897ab9bf286725cdb36c5167ae3e2f39ed55f55ab0c449fe5a10
   0b7706cfa63ad122d9ff7b5f3c3748005bced5b76c43d7471681b88f144e9682a
   c627a2c3639b37800d5c5d7e3cc8eea9689ad018b615ef99f3fced67508
   token_response: 42fd01000102365db273ac96ac0f7806b2d8d0fc09a629e3d
   a5ef1111f8ce56dc80c64480305ead1f810bdb6297adce2852e099e5c40eae18b
   4f9fc8b4e2c214e0a10e50a06e76fd6889281449a7b47521735222137f286a1a1
   5e2c760a015943511eb6eba92eb7472cd0371b79ba82ae8ab98c4097d97d7bbf9
   4fc3cfb9d9b5384fdffc86c430360205c03772817544a5bc66fbb42c01000217b
   186a465203f57e6843f1c57ad5522a1c94665d01cf3e1842e1a935e2bb18d0840
   ab25afd9824b8f1cf35b9908729f9d8192b7397fd4e1ac1814ac1c8705f92e99a
   1281abfc778cea3c52201e6b7e2965e1e2bbf3d9b7111ac86efbd489905fd8ed3
   7ce9833d7b40a70b6ed74548a55f478404c6e00d13324dbd084f68fbc0493eca7
   55c5c6eca6990aaa8e8c2c574ba89fbe75e066e61729a37f021af5dec00a7adf0
   a8ca5a5dc31383de61e94fdc1992a25638541cad8a1b3c8be5511fb9d5ab6e721
   3b621e80cf85ee5c074b35a603edf7715bc475a5074c9090dce16508914d825df
   23b0b00c941f5e1918dd93739e010bda451011d5b691d0a3c940bc010005b2b09
   a6fbf81dde2a58a8b6493e99d1643f91314b6652a86a0fb924e2e8f6a7e124c7b
   f9a66f170715dfa83a9569141d18573133bbf613608d07684b14fdab02e79e64f
   23dd8730fb05dedd270018f91c55c0b58e12a8ff04e0ad9ab88c3360c0100024d
   a2de3b1d3966eb4bca00117068e7a82e993c10fdc5e52d8c38b5e72d398d9b201
   bd26ba2ca117e92cf31b0726aa696c66f8adb16d39afbc9cfbe7b0c0077b78489
   dd5497d821397b70f9856247a59419ae99e84870503ba290d66f42e400fb460ea
   0f8a8a8eb58c5f150b812e48648c1aca1d448066ae1af9cea911591a8af7350e8
   df4ca90fba4d3c4229713f684d0e47b25e178f308120116d2f41a1fc1293fb068
   2d0e9c25139574410c6976be43349846aaaf30fcd029bec0f23d4f564e310652c
   1de6d90397b5478678d7ce37e5d09a8cc5e3a4d593c36095c6da2438c0eab98f2
   15d3e3852a5bb7c099cd155c2a38fa310ebdecc4a93a98a6a79abe9
```

Authors' Addresses

Raphael Robert
Phoenix R&D
Email: ietf@raphaelrobert.com

Christopher A. Wood
Cloudflare
Email: caw@heapingbits.net

Thibault Meunier
Cloudflare Inc.
Email: ot-ietf@thibault.uk