IEEE P802.11
Wireless LANs

|  |
| --- |
| Finding PWE in Constant-Time |
| Date: 2019-09-17 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE | 3333 Scott boulevardSanta Clara, California, United States of America | +1 408 555 1212 |  |
| Jouni Malinen | Qualcomm |  |  |  |
| Mike Montemurro | Blackberry |  |  |  |

Abstract

The countermeasures against side channel attack that SAE puts into the hunting and pecking loop is inefficient and fragile. Recent attacks—e.g. Dragonblood—underscore this problem. A deterministic method that is computable in constant-time without repetitive looping should be used to discover PWE. Do to the minimal number of restrictions on curve type, an appealing way of hashing to an elliptic curve is the Simplified Shallue-Woestijne-Ulas (SSWU) method. For Finite Field Cryptography (FFC) groups, the branching and looping should be removed in order to generate an FFC PWE directly. In addition, it’s important to add detection of group downgrade to SAE.

**Discussion**: SAE requires use of a secret element, PWE, discovered in an agreed upon finite cyclic group. Due to the way the key exchange was initially developed, this PWE discovery cannot be done before the SAE protocol starts.

This element is deterministically discovered by repeatedly hashing the password with some additional information until the resulting hash is the abscissa of a point on the elliptic curve (for ECC) or by exponentiating the hash digest to a constant to produce an element (for FFC). Both of these techniques are prone to side channel attack. While much work has gone into countermeasures to mitigate these attacks, for instance looping 40 times regardless of how soon an abscissa is found, the countermeasures render the whole method of PWE discovery inefficient and very fragile.

When a group is rejected, another one is tried. A man-in-the-middle could exploit this to do a downgrade attack where “good” groups are rejected by the attacker until a “not so good” group is offered which is allowed to go through. There is no way to detect this attack.

**Proposal**: For ECC, use the Simplified Shallue-Woestijne-Ulas (SSWU), as defined in draft-irtf-cfrg-hash-to-curve, to directly hash-to-curve. This method will work for any Weierstrass curve which makes it ideal for use with SAE.

Since SSWU does not generate all points on the elliptic curve, the SSWU method by itself could not be used with the current SAE security proof in the random oracle model. Therefore, the SSWU method is enhanced by the following technique from Brier et al to hash to a password-based element, PT:

 PT(m) := SSWU(h1(m)) + SSWU(h2(m))

Where *m* is the information being hashed, *h1*() and *h2*() are random oracles based on a hash function, and ‘+’ is the element operator (*i.e*., point arithmetic) for ECC.

For FFC groups, the results of the hash will be reduced modulo the prime to produce PT instead of skipping values that would be larger than the prime when interpreted as an integer. No looping is needed.

The secret element, PT, can be computed when the password is provisioned and retained until SAE begins at which time it can be combined with the peer’s MAC addresses to create a session-specific PWE for SAE. Such an approach not only allows for hashing-to-element to be implemented in constant-time; it also helps to avoid timing attacks for implementations that cannot be completely constant-time.

The Simplified SWU method is defined in draft-ietf-cfrg-hash-to-curve. Since this is an Internet-Draft and normative references to such memos are not appropriate (due to their transient nature) the algorithm from the Internet-Draft is copied here. If the draft is advanced to RFC status prior to Draft P802.11REVmd being published this can be changed to include a reference the RFC and the explicit math for SSWU and the calculations of parameter z can be removed in favor of reference to the RFC. At that time IETF downref procedures will have to be followed since we will have a normative reference to an Informational RFC (similar to what we have with RFC 2104 which describes HMAC).

These new techniques are not backwards compatible with the “hunting-and-pecking” loop in the standard and therefore must be signalled as new capabilities. This signalling is compounded by two things: SAE happens before association, and selection of PWE happens before any transactional frames have been sent. Since SAE happens before association, it’s not possible to use an AKM. So support of this is signalled by an AP using a bit in the Extended Capabilities field. Since the SAE protocol itself is not being changed the signalling to use this new PWE discovery method has to be as unintrusive as possible. Therefore, it is signalled with a new status code in the SAE Commit message—“I’m hashing directly to PWE!”. Everything else in SAE (state machine, message formats, computation, message construction and processing, etc) remains the same.

To detect a group downgrade, each peer appends rejected groups to its next Commit message. A concatenation of both sides’ lists of rejected groups (one or both can, of course, be null) is passed as salt to the key derivation function. This ensures that both sides will agree on the same key if there is no man-in-the-middle fiddling with SAE Commit messages. If there is a man-in-the-middle the SAE exchange will fail.

**Changes necessary from D2.3:**

*Note to editor: In the references and most publications, the term “constant-time” seems to be used with a hyphen. This document reflects that. Please use the term as it would conform to the IEEE style guide.*

*Instruct the editor to obtain values from ANA for <ANA-1>, <ANA-2>, and <ANA-3> and to replace all occurances of these placeholders with the real values throughout.*

*Instruct the editor to add the following line to section 2:*

**2. Normative references**

IETF RFC 5869, HMAC-based Extract and Expand Key Derivation Function, H. Krawczyk, P. Eronen, May 2010

*Instruct the editor to modify table 9-42 as indicated:*

 **Table 9-42—Authentication frame body**

|  |  |  |
| --- | --- | --- |
|  **Order** |   **Information** |  **Notes** |
|  23 |  Rejected Groups | The Rejected Groups element is present only in certain Authentication frames as defined in Table 9-43 (Presence of fields and elements in Authentication frames) |

*Instruct editor to modify table 9-43 as indicated:*

 **Table 9-43—Presence of fields and elements in Authentication frames**

|  |  |  |  |
| --- | --- | --- | --- |
| **Authentication Algorithm** | **Authentication transaction sequence number** |  **Status Code** |  **Presence of fields 4 onwards** |
| SAE |  1 |  Any | The Scalar field is present if the Status Code field is zero or <ANA-1>.The FFE field is present if the Status Code field is zero or <ANA-1>.The Anti-Clogging Token field is present if status is 76 or <ANA-1> or if the Authentication frame is in response to a previous rejection with Status 76 or <ANA-1>.The Finite Cyclic Group field is present if the Status Code field is zero, 76, 77, or <ANA-1>.The Password Identifier element is optionally presentif the Status Code is zero, 123, or <ANA-1>.The Rejected Groups element is conditionally present if the Status Code is <ANA-1>. |

*Instruct the editor to modify table 9-52 as indicated:*

 **Table 9-52—Status codes**

|  |  |  |
| --- | --- | --- |
| **Status code** |  **Name** |  **Meaning** |
|  <ANA-1> | SAE\_HASH\_TO\_ELEMENT | SAE authentication uses direct hashing, instead of looping, to obtain the PWE |
| <ANA-1> + 1-65535 |  Reserved |  |

*Instruct the editor to modify table 9-94 as indicates:*

 **Table 9-94—Element IDs**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  **Element** | **Element ID** |  **Extended ID Extension** |  **Extensible** |  **Fragmentable** |
| Rejected Groups (see 9.4.2.244 (Rejected Groups element)) |  255 |  <ANA-2> |  No |  No |
| Reserved |  255 |  <ANA-2> + 1-255 |  |  |

*Instruct the editor to modify table 9-95 as indicated:*

 **Table 9-95—BSS membership selector value encoding**

|  |  |  |
| --- | --- | --- |
|  **Value** |  **Feature** |  **Interpretation** |
|  123 | SAE Hash to Element Only | Indicates that support for the direct hashing to element technique in SAE is required in order to join the BSS. |

*Instruct the editor to mnodify table 9-133 as indicated:*

 **Table 9-133—AKM suite selectors**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 00-0F-AC  | 8 | SAE authentication or using PMKSAcaching as defined in12.6.10.3  | RSNA key management asdefined in 12.7, PMKSAcaching as defined in12.6.10.3 or authenticatedmesh peering exchange asdefined in 14.5 | Defined in12.7.1.7.2 usingSHA-256 |

*Instruct the editor to modify table 9-322 as indicated:*

 **Table 9-322—Extended RSN Capabilities field**

|  |  |  |
| --- | --- | --- |
|  **Bit** |  **Information** |  **Notes** |
|  <ANA-3> | SAE hash-to-element | The AP supports directly hashing to obtain the PWE instead of looping. See 12.4.4.2.3 and 12.4.4.3.3 |
| <ANA-3> + 1 – (8xn – 1) |  Reserved |  |

*Instruct the editor to add new section 9.4.2.244, and allocate a number to replace XYZ, adjusting subsequent figure numbers as appropriate:*

**9.4.2.244 Rejected Groups element**

The Rejected Groups element lists the finite cyclic groups that have been rejected by a peer for use in SAE. The format of the Rejected Groups element is shown in Figure 9-XYZ.

|  |  |  |  |
| --- | --- | --- | --- |
|  Element ID |  Length  |  Element ID Extension |  Rejected Groups |

Octets: 1 1 1 variable

 **Figure 9-XYZ—Rejected Groups element format**

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).

The Rejected Groups field contains a concatenated list of unsigned 16-bit integers representing finite cyclic groups that have been rejected by a peer in a previous authentication attempt.

*Instruct the editor to modify section 12.4.2 as indicated and assign a number for the new table:*

**12.4.2 Assumptions on SAE**

SAE uses two functions, H and CN, that are instantiated with hash functions in HMAC form. H takes a salt and an input key; CN takes a key, a counter, and a sequence of data. Each piece of data passed to CN is converted to an octet string and concatenated together before being concatenated to the counter and passed, along with the key, to the hash function.

Hash

Hash

HMAC-Hash is a specific hash function in HMAC form and When used with the looping technique described in sections 12.4.4.2.2 and 12.4.4.3.2 , H and CN are instantiated withSHA-256. When used with the direct hashing technique described in 12.4.4.2.3 and 12.4.4.3.3 H and CN are instantiated with a hash function from table 12-abc depending on the size of the prime defining the group being used with SAE:

\

 **Table 12-abc – Hash algorithm based on length of prime**

|  |  |  |
| --- | --- | --- |
|  **ECC prime length** |  **FFC prime length** |  **Hash algorithm** |
|  p <= 256 |  p <= 2048 |  SHA-256 |
|  256 < p <= 384 |  2048 < p <= 3072 |  SHA-384 |
|  384 < p |  3072 < p |  SHA-512 |

*Instruct the editor to modify section 12.4.4.2.2 as indicated:*

**12.4.4.2.2 Generation of the password element with ECC groups by looping**

If the AP does not indicate support for the SAE hash-to-element in its Extended RSN Capabilities field or the SAE initiator does not set Status Code field to SAE\_HASH\_TO\_ELEMENT in its SAE Commit message, the password element of an ECC group (PWE) shall be generated in the following random hunt-and-peck fashion.

*Instruct the editor to add the following new section and a assign number for the new table:*

**12.4.4.2.3 Hash-to-curve generation of the password element with ECC groups**

An SAE peer, e.g. a mesh STA or an AP, indicates support for direct hashing to obtain an ECC password element by setting the SAE hash-to-element bit in the Extended RSN Capabilities field in all Beacon and Probe Response frames. An SAE initiator that has identified a peer that supports this technique (through receipt of Beacon or Probe Response frames) shall derive a secret element, PT, according to the following technique and indicate this by setting the status code in the SAE Commit message to SAE\_HASH\_TO\_ELEMENT. An SAE initiator shall not indicate support for this form of element derivation unless its peer has already signalled support for this method. If an SAE Commit message is received with status code equal to SAE\_HASH\_TO\_ELEMENT the peer shall generate the PWE using the following technique and reply with its own SAE Commit message with status code equal to SAE\_HASH\_TO\_ELEMENT.

The direct hashing technique to derive an element of an ECC group is the Simplified Shallue-Woestijne-Ulas (SSWU) deterministic hash-to-curve method. The SSWU method is called twice with two distinct functions to produce two points on the elliptic curve. The two points are summed to create a secret element PT.

This method works for all Weierstrass elliptic curves whose constants *a* and *b* are both not equal to zero. Other curves shall not be used with this hash-to-curve method.

This hash-to-curve method uses HKDF (RFC 5869) with the hash algorithm taken from Table 12-abc based on the length of the prime of the ECC group to perform both functions. First HKDF-Extract is passed a salt in the form of the SSID for which the password is to be used, the password, and optionally a password identifier to produce and intermediary password seed. The resulting seed is passed to HKDF-Expand to produce two distinct strings using different labels. Both values are reduced modulo *p*, the prime defining the curve, and then passed to SSWU to produce distinct points, *P1* and *P2*, whose sum is *PT*.

This secret PT is stored until needed to generate a session-specific PWE (see 12.4.5.2 (PWE and secret generation)).

Algorithmically, this process is as follows:

 *len =* *olen(p) + ceil(olen(p)/2)*

 *pwd-seed =* HKDF-Extract*(ssid, password [|| identifier])*

 *pwd-value =* HKDF-Expand*(pwd-seed, “SAE Hash to Element u1 P1”, len)*

 *u1 = pwd-value modulo p*

 *P1 =* SSWU*(u1)*

 *pwd-value =* HKDF-Expand*(pwd-seed, “SAE Hash to Element u2 P2”, len)*

 *u2 = pwd-value modulo p*

 *P2 =* SSWU*(u2)*

 *PT =* elem-op*(P1, P2)*

where

* HKDF-Extract() and HKDF-Expand() are the functions defined in RFC 5869 instantiated with the hash algorithm from Table 12-abc (Hash algorithm based on prime length))
* ssid is an octet string that represents the SSID with which the password is to be used
* olen() returns the length of its argument in octets
* ceil() returns the smallest integer value that is not less than the passed parameter
* [|| identifier] indicates the optional inclusion of a password identifier, if present
* SSWU(u) is a call to the Simple SWU routine passing in parameter u

The SSWU method produces two values, x1, and x2, at least one of which will represent an abscissa of a point on the curve. If x1 is the abscissa, then x1 becomes the x-coordinate otherwise x2 becomes the x-coordinate. The equation of the curve with the x-coordinate produces the square of the y-coordinate which is recovered by taking the square root. The two possible results of the square root are discriminated by checking its least significant bit with the least significant bit of *u*. The result is a point on the curve.

The SSWU method takes a curve-specific parameter, z, which is determined by finding the number that satisfies the following rules, given p, a, and b, from the curve’s domain parameter set:

1. z = n if
	1. n is not a quadratic residue modulo p
	2. (b/(n\*a)3 + a \* (b/(n\*a)) + b is a quadratic residue modulo p
2. z = -n if
	1. -n is not a quadratic residue modulo p
	2. (b/(-n\*a)3 + a \* (b/(-n\*a)) + b is a quadratic residue modulo p
3. there is no other number n’ that satisfies the above two criteria such that the absolute value of n’ is less than the absolute value of n; and
4. if both n and -n satisfy the above criteria then z is n, the positive value

Values for some defined groups based on their IANA-assigned values are listed in Table 12-xyz:

 **Table 12-xyz—Unique curve parameter**

|  |  |  |
| --- | --- | --- |
|  **Curve name** | **IANA value** |  **z** |
|  NIST p256 |  19 |  -2 |
|  NIST p384 |  20  |  -2 |
|  NIST p521 |  21 |  -2 |
|  NIST p192 |  25 |  -5 |
|  NIST p224 |  26 |  -11 |
| Brainpool p256 |  28 |  -2 |
| Brainpool p384 |  29 |  -5 |
| Brainpool p512 |  30 |  2 |

Algorithmically, the Simplified SWU method is:

*SSWU(u) {*

 *m = (z2 \* u4 + z \* u2) modulo p*

 *l = CEQ(m, 0)*

 *t = inverse(m)*

 *x1 = CSEL(l, (b / (z \* a) modulo p), ((-b/a) \* (1 + t)) modulo p)*

 *gx1 = (x13 + a \* x1 + b) modulo p*

 *x2 = (z \* u2 \* x1) modulo p*

 *gx2 = (x23 + a \* x2 + b) modulo p*

 *l = gx1 is a quadratic residue modulo p*

 *v = CSEL(l, gx1, gx2)*

 *x = CSEL(l, x1, x2)*

 *y = sqrt(v)*

 *l = CEQ(LSB(u), LSB(y))*

 *P = CSEL(l, (x,y), (x, p-y))*

 *output P*

*}*

where:

* p, a, and b are all defined in the domain parameter set for the curve.
* z is a curve-specific parameter from Table 12-xyz
* inverse(x) is calculated as x(p-2) modulo p
* x is a quadratic residue if x((p-1)/2) modulo p is zero or one
* LSB(x) returns the least significant bit of x
* CSEL(x,y,z) operates in constant-time and returns y if x is true and z otherwise.
* CEQ(x,y) operates in constant-time and returns true if x equals y and false otherwise.

All operations in the SSWU algorithm shall be done in constant-time.

Note—For curves based on a prime, p, such that p = 3 mod 4 the square root can be implemented with a single modular exponentiation of (p+1)/4, that is sqrt(w) = w(p+1)/4 modulo p.

*Instruct the editor to modify section 12.4.4.3.2 as indicated:*

**12.4.4.3.2 Generation of the password element with FFC groups by looping**

If the AP does not indicate support for the SAE hash-to-element in its Extended RSN Capabilities field or the SAE initiator does not set Status Code field to SAE\_HASH\_TO\_ELEMENT in its SAE Commit message, the password element of an FFC group (**PWE**) shall be generated in the following random hunt-and-peck fashion.

*Instruct the editor to add the following new section:*

**12.4.4.3.3 Direct Generation of the password element with FFC groups**

An SAE peer indicates support for direct hashing to obtain the FFC password element by setting the SAE hash-to-PWE bit in the Extended RSN Capabilities field in all Beacon and Probe Response frames. An SAE initiator that has identified a peer that supports the following technique (through receipt of Beacon or Probe Response frames) shall derive PT according to the following technique and indicate this by setting the status code in the SAE Commit message to SAE\_HASH\_TO\_ELEMENT. An SAE initiator shall not indicate support for this form of PWE derivation unless its peer has already signalled support. If an SAE Commit message is received with status code equal to SAE\_HASH\_TO\_ELEMENT the peer shall generate the PWE using the following technique and reply with its own SAE Commit message with status code set to SAE\_HASH\_TO\_ELEMENT.

This direct hashing technique uses HKDF (RFC 5869) with the hash algorithm taken from Table 12-abc based on the length of the prime of the FFC group.

To perform this direct hashing technique, HKDF (RFC 5869) is passed a salt in the form of the SSID for which the password is to be used, the password, optionally a password identifier, as an input key, a constant label “SAE Hash to Element”, and the length of the prime to produce a password value. The resulting password value shall be reduced into a range such that 1 < pwd-value < p. Then, it shall be raised to the power (p–1) / q and reduced modulo p (where *p* is the prime number and *q* is the order). This will ensure PT is a generator of order either 1 (if PT=1) or q (for all other values). The probability of PT taking the value 1 is negligible.

This secret PT is stored until needed to generate a session-specific PWE.

Algorithmically, this process is as follows:

 *len =* *olen(p) + ceil(olen(p)/2)*

 *pwd-seed =* HKDF-Extract*(ssid, password [|| identifier])*

 *pwd-value =* HKDF-Expand*(pwd-seed, “SAE Hash to Element”, len)*

 *pwd-value = (pwd-value modulo (p-2)) + 2*

 *PT = pwd-value(p-1)/q modulo p*

where

* HKDF-Extract() and HKDF-Expand() are defined in RFC 5869, instantiated with the hash algorithm identified Table 12-abc (Hash algorithm based on length of prime))
* ssid is an octet string that represents the SSID with which the password is to be used
* olen() returns the length of its argument in octets
* ceil() is the ceiling function that returns the largest whole integer that represents the passed parameter
* [|| identifier] indicates the optional inclusion of a password identifier, if present.
* p and q are defined in the domain parameter set for the group.

This secret PT is stored until needed to generate a session-specific PWE (see 12.4.5.2 (PWE and secret generation)).

*Instruct the editor to modify section 12.4.5.2 as indicated:*

**12.4.5.2 PWE and secret generation**

Prior to beginning the protocol message exchange, the secret element PWE and two secret values are generated.

When a STA supports directly hashing to a group element (according to 12.4.4.2.3 or 12.4.4.3.3) it computes a secret element, PT, off-line at provisioning time for all groups it wishes to support with that password. Prior to initiating SAE to a STA which also supports the direct form of hashing to a group element, or upon receipt of an SAE Commit message indicating it was generated using a direct form of hashing to a group element, it shall generate the PWE by hashing the two peer MAC addresses to produce a digest, reducing the digest modulo the order of the particular group, q, interpreting the reduced digest as an integer and using it with the secret element to generate the PWE:

 *val = H(0n, MAX(STA-A-MAC, STA-B-MAC) || MIN(STA-A-MAC, STA-B-MAC))*

 *val = val modulo (q – 1) + 1*

 *PWE = scalar-op(val, PT)*

where:

* 0n is a salt of all zeros whose length equals the length of the digest from the hash function used to instantiate H() (see table 12-abc in 12.4.2 (Assumptions on SAE))

If a STA does not support a direct form of hashing to a group element it generates the PWE after selecting a group , either the most preferred group if the STA is initiating SAE to a peer, or the group from a received SAE Commit message if the STA is responding to a peer. The PWE shall be generated for that group (according to 12.4.4.2.2 (Generation of the password element with ECC groups) or 12.4.4.3.2 (Generation of the password element with FFC groups), depending on whether the group is ECC or FFC, respectively) using the identities of the two STAs and the configured password.

After generation of the PWE, each STA shall generate a secret value, rand, and a temporary secret value, mask, each of which shall be chosen randomly such that 1 < rand < r and 1 < mask < r and (rand + mask ) mod r is greater than 1, where r is the (prime) order of the group. If their sum modulo r is not greater than 1, they shall both be irretrievably deleted and new values shall be randomly generated. The values rand and mask shall be random numbers produced from a quality random number drawn from a uniform distribution generator. These values shall never be reused on distinct protocol runs.

*Instruct the editor to modify section 12.4.5.4 as indicated:*

**12.4.5.4 Processing of a peer’s SAE Commit message**

If the peer’s SAE Commit message contains a password identifier, the value of that identifier shall be used in construction of the password element (PWE) for this exchange. If a password identifier is present in the peer’s SAE Commit message and there is no password with the given identifier a STA shall fail authentication.

If the peer’s SAE Commit message contains a Rejected Groups element, the list of rejected groups shall be checked to ensure that all of the groups in the list are groups that would be rejected. If any groups in the list would not be rejected then processing of the SAE Commit message terminates and the STA shall reject the peer’s authentication. While the rejected groups are appended to the Rejected Groups element as they are rejected (see 12.4.7.4 (Encoding and decoding of SAE Commit messages)) there is no inherent order to the groups in the list. The order in which they are sent and received shall be retained when deriving keys.

Upon receipt of a peer’s SAE Commit message both the scalar and element shall be verified.

If the scalar value is greater than 1 and less than the order, r , of the negotiated group, scalar validation succeeds; otherwise, it fails. Element validation depends on the type of group. For FFC groups, the element shall be an integer greater than 1 and less than the prime number p minus 1, (p – 1), and the scalar operation of the element and the order of the group, r , shall equal 1 modulo the prime number p . If either of these conditions does not hold, element validation fails; otherwise, it succeeds. For ECC groups, both the x- and y-coordinates of the element shall be non-negative integers less than the prime number p, and the two coordinates shall produce a valid point on the curve satisfying the group’s curve definition, not being equal to the “point at the infinity.” If either of those conditions does not hold, element validation fails; otherwise, element validation succeeds.

If either scalar validation or element validation fails, the STA shall reject the peer’s authentication. If both the scalar and element from the peer’s SAE Commit message are successfully validated, a shared secret element, K , shall be derived using the scalar and element (peer-commit-scalar and ***PEER-COMMITELEMENT*** , respectively) from the peer’s SAE Commit message and the STA’s secret value.

 ***K*** = scalar-op(rand , (elem-op(scalar-op(peer-commit-scalar , ***PWE***),

***PEER-COMMIT-ELEMENT***)))

If the shared secret element, ***K***, is the identity element for the negotiated group (the value one for an FFC group or the point-at-infinity for an ECC group) the STA shall reject the peer’s authentication. Otherwise, a secret value, k , shall be computed as:

k = F(K )

The entropy of k shall then be extracted using H to produce keyseed. The key derivation function from 12.7.1.6.2 (Key derivation function (KDF)) shall then be used with the hash algorithm identified by the AKM suite selector (see Table 9-151 (AKM suite selectors)) to derive a key confirmation key, KCK, and a pairwise master key, PMK, from keyseed. When used with the looping method of PWE generation (see 12.h4.4.2.2 and 12.4.4.3.2), both the KCK and PMK shall be 256 bits in length,. When used with AKMs 00:0F:AC-8 or 00:0F:AC-9 and the direct hashing technique of PWE generation (see 12.4.4.2.3 and 12.4.4.3.3), the KCK shall be the length of the digest generated by H() and the PMK shall be 256 bits in length. Use of other AKMs with the direct hashing technique will require definition of the length of the PMK. When both SAE Commit messages indicated a status code of SAE\_HASH\_TO\_ELEMENT a salt is passed to the KDF consisting of a concatenation of the rejected groups from each peer’s Rejected Groups element; those of the peer with the highest MAC address go first (if only one sent a Rejected Groups element then the salt will consist of that list). If neither peer sent a Rejected Groups element or the status code was not SAE\_HASH\_TO\_ELEMENT the salt shall consist of a series of octets of the value zero whose length equals the length of the digest of the hash function used to instantiate H().

*keyseed = H(salt, k)*

*kck\_and\_pmk = KDF-Hash-Length(keyseed, “SAE KCK and PMK”,*

*(commit-scalar + peer-commit-scalar) mod r)*

*KCK = L(kck\_and\_pmk, 0, Q)*

*PMK = L(kck\_and\_pmk, Q, 256)*

where

* *salt* is either a series of 0 octets or a list of rejected groups (see 12.4.7.4 (Encoding and decoding of SAE Commit messages)).
* *KDF-Hash-Length* is the key derivation function defined in 12.7.1.6.2 (Key derivation function (KDF)) using the hash algorithm defined for H())).
* *Q* is the length of the digest of the H(), the hash function used
* *Length* is Q plus 256

*Instruct the editor to modify section 12.4.7.4 as indicated:*

**12.4.7.4 Encoding and decoding of SAE Commit messages**

An SAE Commit message shall be encoded as an Authentication frame with an Authentication Algorithm

Number field set to 3, a Transaction Sequence Number of 1 and a Status Code of SUCCESS or SAE\_HASH\_TO\_ELEMENT. Status codes not equal to SUCCESS or SAE\_HASH\_TO\_ELEMENT indicate a rejection of a peer’s SAE Commit message and are described in 12.4.7.6 (Status codes).

An SAE Commit message shall consist of a Finite Cyclic Group field (9.4.1.42 (Finite Cyclic Group field)) indicating a group, a Scalar field (9.4.1.39 (Scalar field)) containing the scalar, and an FFE field containing the element (9.4.1.40 (FFE field)). If the SAE Commit message is in response to an Anti-Clogging Token field request (see 12.4.7.6 (Status codes)), the Anti-Clogging Token field is present (see 9.4.1.38 (Anti-Clogging Token field)). If a password identifier is used in generation of the password element (PWE) the Password identifier element shall be present and the identifier shall be encoded as a UTF-8 string in the Identifier portion of the element (see 9.4.2.216 (Password Identifier element)). If an SAE Commit message with status code equal to SAE\_HASH\_TO\_ELEMENT is being sent in response to rejection of a previous SAE Commit message with status set to UNSUPPORTED\_FINITE\_CYCLIC\_GROUP, the group that was rejected shall be appended, after the rejected groups from previous attempts if applicable, to the Rejected Groups field of the Rejected Groups element. Each rejected group shall be represented as an unsigned 16-bit integer using the bit ordering conventions of 9.2.2 (Conventions).

*Instruct the editor to modify section 12.4.7.6 as indicated:*

**12.4.7.6 Status codes**

An SAE Commit message with a status code not equal to SUCCESS or SAE\_HASH\_TO\_ELEMENT shall indicate that a peer rejects a previously sent SAE Commit message. An unsupported finite cyclic group is indicated with a status code of UNSUPPORTED\_FINITE\_CYCLIC\_GROUP, “Authentication is rejected because the offered finite cyclic group is not supported.” An unknown password identifier is indicated with a status code of UNKNOWN\_PASSWORD\_IDENTIFER, “Authentication is rejected because the password identifier is unknown.” An Anti-Clogging Token field is requested by transmitting an SAE Commit message with a status code of ANTI\_CLOGGING\_TOKEN\_REQUIRED, “Anti-Clogging Token Requested,” with the Anti-Clogging Token field occupying the Token field of the Authentication frame.

*Instruct the editor to append the following to section J.10:*

Hash to Curve technique of PT/PWE Generation

group 19

SSID: byteme

identifier: psk4internet

password: mekmitasdigoat

MAC address 1: 3b:36:c2:8b:83:03

MAC address 2: 58:36:c0:64:2d:31

------------------------------------------------------------------------

calculating PT for group 19

salt:

62797465 6d65

ikm:

6d656b6d 69746173 6469676f 61747073 6b34696e 7465726e 6574

prk:

3bd53fe9 223dc028 0fbfce17 d7a35640 64e20f48 c6ec7224 6ce367b5 569a22af

info:

53414520 48617368 20746f20 456c656d 656e7420 75312050 31

okm:

a5044469 ab16f25b 6abf1e0e 37a36b56 f50be733 69053df8 db87989a 6b66fd1a

491f1cda cbd07931 620f8300 8ffc0ecc

SSWU(u1)

--------

u1:

dc941bc3 c6a2b494 8b6c61d5 5590ecb1 f0c51c4b 1bebaff6 77e59369 8d5a53c6

m = z^2 \* u^4 + z \* u^2:

fad7d90d 0364a7df b6e6f7ed cf579efe 962abfaf 1f6267c3 7ea53c05 7853191b

t = 1/m:

a0737c9e badedd9e f31e13e2 a813e02c c19d3673 ae561679 fc93476a 6c8be5cc

(-b/a) \* (1 + t):

c39e7523 2f8f0e09 e1c3b369 98d6201a 193d407b 82b6a830 77d5a31f d189ffda

b/(z \* a):

39cbb3a3 f1b46dfc 1dfc9f8e 3e6ec11f 662f811d a20df2d3 b4a25f5f b14dbab7

m != 0, so x1 == (-b/a)\*(1+t)

x1:

c39e7523 2f8f0e09 e1c3b369 98d6201a 193d407b 82b6a830 77d5a31f d189ffda

gx1:

df2d0cf0 f7734200 1cc39feb e0200ed9 69df62d8 a17105ff 50cf9c39 126a1bd2

x2:

d92b5a04 a91b2b14 a6b44a9e 16b9bda3 e17cd1c2 c68e71dd ec368631 8ba747b9

gx2:

4219464e db1af3b3 58e0afde fb682339 cee7ff82 61ed5a12 b0694e9e 302d6096

gx1 is a quadratic residue

gx2 is not a quadratic residue

point P1...

x:

c39e7523 2f8f0e09 e1c3b369 98d6201a 193d407b 82b6a830 77d5a31f d189ffda

y:

5314ad54 c895082c 25378bd7 4179f360 9aefebdc 39b0a8dd 163b169d 3a63f2f0

-----------------------------------

salt:

62797465 6d65

ikm:

6d656b6d 69746173 6469676f 61747073 6b34696e 7465726e 6574

prk:

3bd53fe9 223dc028 0fbfce17 d7a35640 64e20f48 c6ec7224 6ce367b5 569a22af

info:

53414520 48617368 20746f20 456c656d 656e7420 75322050 32

okm:

9b4e0d5b 1879f253 c5319615 099b05ae c5b06fa5 e788bcfd 1e9ea60d 33436927

190814c3 22a62585 c93c577b baa3d307

u2:

1b8375a5 18bc2139 6ad6a65e 5597e0bf 80d793b6 d66e2534 a6e7dfe3 ee22616f

SSWU(u2)

--------

m = z^2 \* u^4 + z \* u^2:

db17e7b8 bb6b6044 e5be8388 b3e4f2b3 550c3a98 5f2ee976 75925364 2eb610a2

t = 1/m:

23c000c3 c4d3e565 d5277699 1fbd56b0 2d5bfee3 64a3dba8 493600f1 96bce53a

(-b/a) \* (1 + t):

ca2a7add 61e3e268 16136ff5 da108f89 b0e5f233 62effb64 5c0d6319 6a49e5ea

b/(z \* a):

39cbb3a3 f1b46dfc 1dfc9f8e 3e6ec11f 662f811d a20df2d3 b4a25f5f b14dbab7

m != 0, so x1 == (-b/a)\*(1+t)

x1:

ca2a7add 61e3e268 16136ff5 da108f89 b0e5f233 62effb64 5c0d6319 6a49e5ea

gx1:

193fae40 a2427128 ca0840e6 ef07aea5 bd5078e9 a9214dbb d2abe7a5 d9930b25

x2:

ad929df7 1d34ee5f 29d8cbca 824b66a5 4e187952 a5172d3b c191691f 951c713f

gx2:

21b7680c eeb4f3fa e94373b0 95b64694 d1fee6b0 a54bff1d a95eab06 aa624c4b

gx1 is not a quadratic residue

gx2 is a quadratic residue

point P2...

x:

ad929df7 1d34ee5f 29d8cbca 824b66a5 4e187952 a5172d3b c191691f 951c713f

y:

f79f6ee4 399ba75c 5c6a128c 7552688f 35bbed3d 16440795 6e57e9f1 9a6e2649

-----------------------------------

PT = P1 + P2:

x:

7bbba151 1f5df8b7 adf0735f 660a0338 dcfbf22c a953c085 7f266317 faeb17d6

y:

f375dafd 411ec750 e37a6ea1 1a74e7ea 81ad6a61 18436a76 d3f12898 bc038fdc

val:

a461dc7c 57a4024e 719f321c 082ace5e 0f8fcf5c 0b86109b 14796714 abfd1347

PWE = val \* PE:

x:

19d337c9 30792b47 2b145fc1 5b98640a 0e7d3bb0 7dc0adee 6fc9df75 dec2d694

y:

b78a0239 2029e7f4 52413d35 8c88d916 c890ba40 d993e32d d00ffb58 ee627498

**References:**

Brier E., Coron JS., Icart T., Madore D., Randriam H., Tibouchi M. (2010) “Efficient Indifferentiable Hashing into Ordinary Elliptic Curves.” In: Rabin T. (eds) Advances in Cryptology – CRYPTO 2010. Lecture Notes in Computer Science, vol 6223. Springer, 2010

Shallue, A. and van de Woestijne, C, “Construction of rational points on elliptic curves over finite fields”, Lecture Notes in Computer Science, vol 4076, pages 510-524, Springer, 2006.

Ulas, M., “Rational points on certain hyperelliptic curves over finite fields.”, Polish Academy of Sciences, 55(2): 97-104, 2007

Wahby, R. and Boneh, D., “Fast and simple constant-time hashing to the BLS12-381 elliptic curve”, Cryptology ePrint Archive, Report 2019/403, 2019.

Faz-Hernandez, A., Scott, S., Sullivan, N., Wahby, R., Wood, C., “Hashing to Elliptic Curves”, draft-irtf-cfrg-hash-to-curve, A work in progress, July 2019

Krawczyk, H., Eronen, P., “HMAC-based Extract and Expand Key Derivation Function (HKDF)”, RFC 5869, May 2010