keyprov
Internet-Draft
Intended status: Informational
Expires: June 27, 2009

P. Hoyer
ActivIdentity
M. Pei
VeriSign
S. Machani
Diversinet
A. Doherty
RSA, The Security Division of EMC

December 24, 2008

Additional Portable Symmetric Key Container (PSKC) Algorithm Profiles
draft-hoyer-keyprov-pskc-algorithm-profiles-00.txt

Status of this Memo

Copyright Notice

Abstract

The Portable Symmetric Key Container (PSKC) contains a number of XML elements and XML attributes carrying keys and related information. Not all algorithms, however, are able to use all elements and for other algorithm certain information is mandatory. This lead to the introduction of PSKC algorithm profiles that provide further description about the mandatory and optional information elements and their semantic, including extensions that may be needed. The main PSKC specification defines two PSKC algorithm profiles, namely "HOTP" and "PIN". This document extends the initial set and specifies nine further algorithm profiles for PKSC.

Table of Contents

1. Introduction

This document specifies a set of algorithm profiles for PKSC, namely

OCRA (OATH Challenge Response Algorithm)

TOTP (OATH Time based OTP)

SecurID-AES

SecurID-AES-Counter

SecurID-ALGOR

ActivIdentity-3DES

ActivIdentity-AES

ActivIdentity-DES

ActivIdentity-EVENT

[Editor's Note: The content of this document was created by moving a number of PSKC algorithm profiles from draft-ietf-keyprov-portable-symmetric-key-container-06.txt into this document. Since draft-ietf-keyprov-portable-symmetric-key-container-07.txt had experienced a number of changes the description and the examples in this document are likely to be out-of-sync. Re-alignment will be provided in a future version.]

2. Terminology

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

3. OCRA (OATH Challenge Response Algorithm)

Common Name: OCRA

Class: OTP

URI: http://www.ietf.org/keyprov/pskc#OCRA-1:(ocra_suite_parameters) - e.g. http://www.ietf.org/keyprov/pskc#OCRA-1:HOTP-SHA512-8:C-QN08

Algorithm Definition: http://www.ietf.org/internet-drafts/draft-mraihi-mutual-oath-hotp-variants-07.txt

Identifier Definition (this RFC)

Registrant Contact: IESG

Profile of XML attributes and subelements of the <Key> entity:

For a <Key> of this algorithm, the <Usage> subelements MUST be present. The "CR" attribute of the <Usage> MUST be set "true" and it MUST be the only attribute set. The element <ChallengeFormat>

and <ResponseFormat> of the <Usage> MUST be present.

For the <Data> elements of a <Key> of this algorithm, the following subelements MUST be present in either the <Key> element itself or an commonly shared <KeyProperties> element.

* Counter

* Time

If the element <Time> is present, the following elements MUST be also present.

* TimeInterval

The following additional constraints apply:

- The value of the <Secret> element MUST contain key material with a lengthy of at least 16 octets (128 bits) if it is present.

- The <ResponseFormat> element MUST have the 'Format' attribute set to "DECIMAL", and the 'Length' attribute MUST be between 6 and 9.

- The <PINPolicy> element MAY be present but the <Format> child element of the <PINPolicy> element cannot be set to "Algorithmic".

An example of a <Key> of this algorithm is as follows.

```
<?xml version="1.0" encoding="UTF-8"?>
<KeyContainer Version="1.0"
xmlns="urn:ietf:params:xml:ns:keyprov:pskc:1.0">
    <Device>
        <DeviceInfo>
            <Manufacturer>TokenVendorAcme</Manufacturer>
            <SerialNo>987654322</SerialNo>
        </DeviceInfo>
```

```
          <Key KeyId="12345678"
          KeyAlgorithm="http://www.ietf.org/keyprov/
          pskc#OCRA-1:HOTP-SHA512-8:C-QN08">
              <Issuer>Issuer</Issuer>
              <Usage CR="true">
                <ChallengeFormat Min="8" Max="8" Format="DECIMAL"/>
                <ResponseFormat Length="8" Format="DECIMAL"/>
              </Usage>
              <Data>
                <Secret>
                   <PlainValue>MTIzNDU2Nzg5MDEyMzQ1Njc4OTA=</PlainValue>
                </Secret>
                <Counter>
                  <PlainValue>0</PlainValue>
                </Counter>
              </Data>
          </Key>
      </Device>
  </KeyContainer>
```


4. TOTP (OATH Time based OTP)

Common Name: TOTP

Class: OTP

URI: http://www.ietf.org/keyprov/pskc#totp

Algorithm Definition: http://www.ietf.org/internet-drafts/draft-mraihi-totp-timebased-00.txt

Identifier Definition (this RFC)

Registrant Contact: IESG

Profile of XML attributes and subelements of the <Key> entity:

For a <Key> of this algorithm, the <Usage> subelements MUST be present. The "OTP" attribute of the <Usage> MUST be set "true" and it MUST be the only attribute set. The element <ResponseFormat> of the <Usage> MUST be used to indicate the OTP length and the value format.

For the <Data> elements of a <Key> of this algorithm, the following subelements MUST be present in either the <Key> element itself or an commonly shared <KeyProperties> element.

* Time

* TimeInterval

The following additional constraints apply:

- The value of the <Secret> element MUST contain key material with a lengthy of at least 16 octets (128 bits) if it is present.

- The <ResponseFormat> element MUST have the 'Format' attribute set to "DECIMAL", and the 'Length' attribute MUST be between 6 and 9.

- The <PINPolicy> element MAY be present but the <Format> child element of the <PINPolicy> element cannot be set to "Algorithmic".

An example of a <Key> of this algorithm is as follows.


```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<KeyContainer Version="1.0"
xmlns="urn:ietf:params:xml:ns:keyprov:pskc:1.0">
    <Device>
        <DeviceInfo>
            <Manufacturer>TokenVendorAcme</Manufacturer>
            <SerialNo>987654323</SerialNo>
        </DeviceInfo>
        <Key KeyAlgorithm="http://www.ietf.org/keyprov/pskc#totp"
        KeyId="987654323">
            <Issuer>Issuer</Issuer>
            <Usage OTP="true">
                <ResponseFormat Length="6" Format="DECIMAL"/>
            </Usage>
            <Data>
                <Secret>
                    <PlainValue>
                    MTIzNDU2Nzg5MDEyMzQ1Njc4OTA=
                    </PlainValue>
                </Secret>
                <Time>
                    <PlainValue>0</PlainValue>
                </Time>
                <TimeInterval>
                    <PlainValue>30</PlainValue>
                </TimeInterval>
                <TimeDrift>
                    <PlainValue>4</PlainValue>
                </TimeDrift>
            </Data>
        </Key>
    </Device>
</KeyContainer>
```

5. SecurID-AES

Common Name: SecurID-AES

Class: OTP

URI: http://www.rsasecurity.com/rsalabs/otps/schemas/2005/09/otps-wst#SecurID-AES

Algorithm Definition: http://www.rsa.com/rsalabs/node.asp?id=2821

Identifier Definition: http://www.rsa.com/rsalabs/node.asp?id=2821

Registrant Contact: Andrea Doherty, RSA the Security Division of EMC, <andrea.doherty@rsa.com>

Profile of XML attributes and subelements of the <Key> entity:

For a <Key> of this algorithm, the <StartDate>, <ExpiryDate>, and <Usage> sub-elements MUST be present. The "OTP" attribute of <Usage> MUST be set to "true" and it MUST be the only attribute set. The <ResponseFormat> sub-element of <Usage> MUST be used to indicate the OTP length and the value format.

The following additional constraints apply:

- The value of the <Secret> element MUST contain key material with a lengthy of at least 16 octets (128 bits) if it is present.

- The <ResponseFormat> element MUST have the 'Format' attribute set to "DECIMAL", and the 'Length' attribute MUST be set to a minimum value of 6.

- The <StartDate> and <ExpiryDate> elements MUST be of type <xs:dateTime>.

- The <PINPolicy> element MAY be present but the <Format> child element of the <PINPolicy> element cannot be set to "Algorithmic".

An example of a <Key> of this algorithm is as follows.

```
<?xml version="1.0" encoding="UTF-8"?>
<KeyContainer Version="1.0"
  xmlns="urn:ietf:params:xml:ns:keyprov:pskc:1.0"
  <Device>
    <DeviceInfo>
      <Manufacturer>RSA, The Security Division of EMC</Manufacturer>
      <SerialNo>123456798</SerialNo>
    </DeviceInfo>
    <Key
      KeyAlgorithm=http://www.rsasecurity.com/rsalabs/otps/schemas/2005
      /09/otps-wst#SecurID-AES
      KeyId="23456789">
      <Issuer>Issuer</Issuer>
      <Usage OTP="true">
        <ResponseFormat Length="6" Format="DECIMAL"/>
      </Usage>
      <StartDate>2006-04-14T00:00:00Z</StartDate>
      <ExpiryDate>2010-09-30T00:00:00Z</ExpiryDate>
    </Key>
  </Device>
</KeyContainer>
```

6. SecurID-AES-Counter

Common Name: SecurID-AES-Counter

Class: OTP

URI: http://www.rsa.com/names/2008/04/algorithms/SecurID/SecurID-AES128-Counter

Algorithm Definition: http://www.rsa.com/names/2008/04/algorithms/SecurID/SecurID-AES128-Counter

Identifier Definition http://www.rsa.com/names/2008/04/algorithms/SecurID/SecurID-AES128-Counter

Registrant Contact: Andrea Doherty, RSA the Security Division of EMC, <andrea.doherty@rsa.com>

Profile of XML attributes and subelements of the <Key> entity:

For a <Key> of this algorithm, the <StartDate>, <ExpiryDate>, and <Usage> sub-elements MUST be present. The "OTP" attribute of <Usage> MUST be set to "true" and it MUST be the only attribute set. The <ResponseFormat> sub-element of <Usage> MUST be used to indicate the OTP length and the value format.

For the Data elements of a <Key> of this algorithm, the following subelements MUST be present in either the <Key> element itself or an commonly shared <KeyProperties> element.

* Counter

The following additional constraints apply:

- The value of the <Secret> element MUST contain key material with a lengthy of at least 16 octets (128 bits) if it is present.

- The <ResponseFormat> element MUST have the 'Format' attribute set to "DECIMAL", and the 'Length' attribute MUST be set to a minimum value of 6.

- The <StartDate> and <ExpiryDate> elements MUST be of type <xs:dateTime>.

- The <PINPolicy> element MAY be present but the <Format> child element of the <PINPolicy> element cannot be set to "Algorithmic".

An example of a <Key> of this algorithm is as follows.

```
<?xml version="1.0" encoding="UTF-8"?>
<KeyContainer Version="1.0"
  xmlns="urn:ietf:params:xml:ns:keyprov:pskc:1.0"
    <Device>
       <DeviceInfo>
          <Manufacturer>RSA, The Security Division of EMC</Manufacturer>
          <SerialNo>123456798</SerialNo>
       </DeviceInfo>
       <Key
          KeyAlgorithm=http://www.rsa.com/names/2008/04/algorithms/
          SecurID/SecurID-AES128-Counter
          KeyId="23456789">
          <Issuer>Issuer</Issuer>
          <Usage OTP="true">
            <ResponseFormat Length="6" Format="DECIMAL"/>
          </Usage>
          <StartDate>2006-04-14T00:00:00Z</StartDate>
          <ExpiryDate>2010-09-30T00:00:00Z</ExpiryDate>
          <Data>
            <Secret>
              <PlainValue>MTIzNDU2Nzg5MDEyMzQ1Njc4OTA=
              </PlainValue>
```

```
            </Secret>
            <Counter>
              <PlainValue>0</PlainValue>
            </Counter>
          </Data>
        </Key>
    </Device>
</KeyContainer>
```


7. SecurID-ALGOR

Common Name: SecurID-ALGOR

Class: OTP

URI: http://www.rsasecurity.com/rsalabs/otps/schemas/2005/09/otps-wst#SecurID-ALGOR

Algorithm Definition: http://www.rsa.com/rsalabs/node.asp?id=2821

Identifier Definition: http://www.rsa.com/rsalabs/node.asp?id=2821

Registrant Contact: Andrea Doherty, RSA the Security Division of EMC, <andrea.doherty@rsa.com>

Profile of XML attributes and subelements of the <Key> entity:

For a <Key> of this algorithm, the <StartDate>, <ExpiryDate>, and <Usage> sub-elements MUST be present. The "OTP" attribute of <Usage> MUST be set to "true" and it MUST be the only attribute set. The <ResponseFormat> sub-element of <Usage> MUST be used to indicate the OTP length and the value format.

The following additional constraints apply:

- The value of the <Secret> element MUST contain key material with a lengthy of at least 8 octets (64 bits) if it is present.

- The <ResponseFormat> element MUST have the 'Format' attribute set to "DECIMAL", and the 'Length' attribute MUST be set to a value of 6 through 8.

- The <StartDate> and <ExpiryDate> elements MUST be of type <xs:dateTime>.

- The <PINPolicy> element MAY be present but the <Format> child element of the <PINPolicy> element cannot be set to "Algorithmic".

An example of a <Key> of this algorithm is as follows.


```
<?xml version="1.0" encoding="UTF-8"?>
<KeyContainer Version="1.0"
xmlns="urn:ietf:params:xml:ns:keyprov:pskc:1.0"
  <Device>
    <DeviceInfo>
      <Manufacturer>RSA, The Security Division of EMC</Manufacturer>
      <SerialNo>123456798</SerialNo>
    </DeviceInfo>
    <Key
        KeyAlgorithm=http://www.rsasecurity.com/rsalabs/otps/schemas/
        2005/09/otps-wst#SecurID-ALGOR KeyId="23456789">
```

```
        <Issuer>Issuer</Issuer>
        <Usage OTP="true>
           <ResponseFormat Length="6" Format="DECIMAL"/>
        </Usage>
        <StartDate>2006-04-14T00:00:00Z</StartDate>
        <ExpiryDate>2010-09-30T00:00:00Z</ExpiryDate>
      </Key>
    </Device>
  </KeyContainer>
```


8. ActivIdentity-3DES

Common Name: ActivIdentity-3DES

Class: OTP

URI: http://www.actividentity.com/2008/04/algorithms/algorithms#ActivIdentity-3DES

Algorithm Definition: http://www.actividentity.com/2008/04/algorithms/algorithms#ActivIdentity-3DES

Identifier Definition http://www.actividentity.com/2008/04/algorithms/algorithms#ActivIdentity-3DES

Registrant Contact: Philip Hoyer, ActivIdentity Inc, <philip.hoyer@actividentity.com>

Profile of XML attributes and subelements of the <Key> entity:

For a <Key> of this algorithm, the <Usage> subelements MUST be present. This algorithm can be used for otp, challenge response, parameter based MACing (integrity) and to generate a device unlock code (n case of devices where there is local PIN management and the devce has been locked after a specific amount of wrong PIN entry attempts). Hence the "OTP", "CR","Integrity" and "Unlock" attribute of the <Usage> can be set to "true", but at least one of the above MUST be set to true. The element <ResponseFormat> of the <Usage> MUST be used to indicate the OTP length, the value format and optionally if a check digit is being used. If the use is challenge-response then the <ChallengeFormat> of the <Usage> MUST be used to indicate the challenge minimum and maximum length, its format and optionally if a check digit is being used.

For the <Data> elements of a <Key> of this algorithm, the following subelements MUST be present in either the <Key> element itself or an commonly shared <KeyProperties> element.

* Secret

* Counter

* Time

* TimeInterval

The following additional constraints apply:

- The value of the <Secret> element MUST contain key material with a length of at least 16 octets (Double DES keys 128 bits including parity) if it is present.

- The <ResponseFormat> element MUST have the 'Format' attribute set to "DECIMAL" or "HEXADECIMAL", and the 'Length' attribute MUST be between 6 and 16.

- The <ChallengeFormat> element MUST have the 'Format' attribute set to "DECIMAL", and the 'Min' and 'Max' attributes be between 4 and 16 (The Min attribute MUST be equal or less than the Max).

- The <PINPolicy> element MAY be present but the <Format> child element of the <PINPolicy> element cannot be set to "Algorithmic".

An example of a Key of this algorithm is as follows.

```
<?xml version="1.0" encoding="UTF-8"?>
<KeyContainer Version="1.0"
xmlns="urn:ietf:params:xml:ns:keyprov:pskc:1.0">
    <Device>
        <DeviceInfo>
            <Manufacturer>ActivIdentity</Manufacturer>
            <SerialNo>34567890</SerialNo>
        </DeviceInfo>
        <Key KeyAlgorithm="http://www.actividentity.com/
        2008/04/algorithms/algorithms#ActivIdentity-3DES"
        KeyId="12345677">
            <Issuer>Issuer</Issuer>
            <Usage OTP="true">
                <ResponseFormat Length="8" Format="DECIMAL"/>
            </Usage>
            <Data>
                <Secret>
                    <PlainValue>
                    MTIzNDU2Nzg5MDEyMzQ1Njc4OTA=
                    </PlainValue>
                </Secret>
                <Counter>
                    <PlainValue>0</PlainValue>
                </Counter>
                <Time>
                    <PlainValue>0</PlainValue>
                </Time>
                <TimeInterval>
                    <PlainValue>32</PlainValue>
                </TimeInterval>
                <TimeDrift>
                    <PlainValue>0</PlainValue>
                </TimeDrift>
            </Data>
        </Key>
    </Device>
</KeyContainer>
```

9. ActivIdentity-AES

Common Name: ActivIdentity-AES

Class: OTP

URI: http://www.actividentity.com/2008/04/algorithms/algorithms#ActivIdentity-AES

Algorithm Definition: http://www.actividentity.com/2008/04/algorithms/algorithms#ActivIdentity-AES

Identifier Definition http://www.actividentity.com/2008/04/algorithms/algorithms#ActivIdentity-AES

Registrant Contact: Philip Hoyer, ActivIdentity Inc, <philip.hoyer@actividentity.com>

Profile of XML attributes and subelements of the <Key> entity:

For a <Key> of this algorithm, the <Usage> subelements MUST be present. This algorithm can be used for otp, challenge response, parameter based MACing (integrity) and to generate a device unlock code (n case of devices where there is local PIN management and the devce has been locked after a specific amount of wrong PIN entry attempts). Hence the "OTP", "CR","Integrity" and "Unlock" attribute of the <Usage> can be set to "true", but at least one of the above MUST be set to true. The element <ResponseFormat> of the <Usage> MUST be used to indicate the OTP length, the value format and optionally if a check digit is being used. If the use is challenge-response then the <ChallengeFormat> of the <Usage> MUST be used to indicate the challenge minimum and maximum length, its format and optionally if a check digit is being used.

For the <Data> elements of a key of this algorithm, the following subelements MUST be present in either the <Key> element itself or an commonly shared <KeyProperties> element.

* Secret

* Counter

* Time

* TimeInterval

The following additional constraints apply:

- The value of the <Secret> element MUST contain key material with a length of at least 16 octets (128 bits) if it is present.

- The <ResponseFormat> element MUST have the 'Format' attribute set to "DECIMAL" or "HEXADECIMAL", and the 'Length' attribute MUST be between 6 and 16.

- The <ChallengeFormat> element MUST have the 'Format' attribute set to "DECIMAL", and the 'Min' and 'Max' attributes be between 4 and 16 (The Min attribute MUST be equal or less than the Max).

- The <PINPolicy> element MAY be present but the <Format> child element of the <PINPolicy> element cannot be set to "Algorithmic".

An example of a <Key> of this algorithm is as follows.

```
<?xml version="1.0" encoding="UTF-8"?>
<KeyContainer Version="1.0"
  xmlns="urn:ietf:params:xml:ns:keyprov:pskc:1.0">
    <Device>
        <DeviceInfo>
            <Manufacturer>ActivIdentity</Manufacturer>
            <SerialNo>34567890</SerialNo>
        </DeviceInfo>
        <Key KeyAlgorithm="http://www.actividentity.com/
        2008/04/algorithms/algorithms#ActivIdentity-AES"
        KeyId="12345677">
            <Issuer>Issuer</Issuer>
            <Usage OTP="true">
                <ResponseFormat Length="8" Format="DECIMAL"/>
            </Usage>
            <Data>
                <Secret>
                    <PlainValue>
                    MTIzNDU2Nzg5MDEyMzQ1Njc4OTA=
```

```
                    </PlainValue>
                </Secret>
                <Counter>
                    <PlainValue>0</PlainValue>
                </Counter>
                <Time>
                    <PlainValue>0</PlainValue>
                </Time>
                <TimeInterval>
                    <PlainValue>32</PlainValue>
                </TimeInterval>
                <TimeDrift>
                    <PlainValue>0</PlainValue>
                </TimeDrift>
            </Data>
        </Key>
    </Device>
</KeyContainer>
```


10. ActivIdentity-DES

Common Name: ActivIdentity-DES

Class: OTP

URI: http://www.actividentity.com/2008/04/algorithms/algorithms#ActivIdentity-DES

Algorithm Definition: http://www.actividentity.com/2008/04/algorithms/algorithms#ActivIdentity-DES

Identifier Definition http://www.actividentity.com/2008/04/algorithms/algorithms#ActivIdentity-DES

Registrant Contact: Philip Hoyer, ActivIdentity Inc, <philip.hoyer@actividentity.com>

Profile of XML attributes and subelements of the <Key> entity:

For a <Key> of this algorithm, the <Usage> subelements MUST be present. This algorithm can be used for otp, challenge response, parameter based MACing (integrity) and to generate a device unlock code (n case of devices where there is local PIN management and the devce has been locked after a specific amount of wrong PIN entry attempts). Hence the "OTP", "CR","Integrity" and "Unlock" attribute of the <Usage> can be set to "true", but at least one of the above MUST be set to true. The element <ResponseFormat> of the <Usage> MUST be used to indicate the OTP length, the value format and optionally if a check digit is being used. If the use is challenge-response then the <ChallengeFormat> of the <Usage> MUST be used to indicate the challenge minimum and maximum length, its format and optionally if a check digit is being used.

For the <Data> elements of a key of this algorithm, the following subelements MUST be present in either the <Key> element itself or an commonly shared <KeyProperties> element.

* Counter

* Time

* TimeInterval

The following additional constraints apply:

- The value of the <Secret> element MUST contain key material with a length of at least 8 octets (56 bits + parity) if it is

present.

- The <ResponseFormat> element MUST have the 'Format' attribute set to "DECIMAL" or "HEXADECIMAL", and the 'Length' attribute MUST be between 6 and 16.

- The <ChallengeFormat> element MUST have the 'Format' attribute set to "DECIMAL", and the 'Min' and 'Max' attributes be between 4 and 16 (The Min attribute MUST be equal or less than the Max).

- The <PINPolicy> element MAY be present but the <Format> child element of the <PINPolicy> element cannot be set to "Algorithmic".

An example of a <Key> of this algorithm is as follows.

```
<?xml version="1.0" encoding="UTF-8"?>
<KeyContainer Version="1.0"
xmlns="urn:ietf:params:xml:ns:keyprov:pskc:1.0">
    <Device>
        <DeviceInfo>
            <Manufacturer>ActivIdentity</Manufacturer>
            <SerialNo>34567890</SerialNo>
        </DeviceInfo>
        <Key KeyAlgorithm="http://www.actividentity.com/
        2008/04/algorithms/algorithms#ActivIdentity-DES"
        KeyId="12345677">
            <Issuer>Issuer</Issuer>
            <Usage OTP="true">
                <ResponseFormat Length="8" Format="DECIMAL"/>
            </Usage>
            <Data>
                <Secret>
                    <PlainValue>
                    MTIzNDU2Nzg5MDEyMzQ1Njc4OTA=
                    </PlainValue>
                </Secret>
                <Counter>
                    <PlainValue>0</PlainValue>
                </Counter>
                <Time>
                    <PlainValue>0</PlainValue>
                </Time>
                <TimeInterval>
                    <PlainValue>32</PlainValue>
                </TimeInterval>
                <TimeDrift>
                    <PlainValue>0</PlainValue>
                </TimeDrift>
            </Data>
        </Key>
    </Device>
</KeyContainer>
```

11. ActivIdentity-EVENT

Common Name: ActivIdentity-EVENT

Class: OTP

URI: http://www.actividentity.com/2008/04/algorithms/algorithms#ActivIdentity-EVENT

Algorithm Definition: http://www.actividentity.com/2008/04/algorithms/algorithms#ActivIdentity-EVENT

Identifier Definition http://www.actividentity.com/2008/04/algorithms/algorithms#ActivIdentity-EVENT

Registrant Contact: Philip Hoyer, ActivIdentity Inc, <philip.hoyer@actividentity.com>

Profile of XML attributes and subelements of the <Key> entity:

For a <Key> of this algorithm, the <Usage> subelements MUST be present. This algorithm can be used for otp, challenge response, parameter based MACing (integrity) and to generate a device unlock code (n case of devices where there is local PIN management and the device has been locked after a specific amount of wrong PIN entry attempts). Hence the "OTP", "CR","Integrity" and "Unlock" attribute of the <Usage> can be set to "true", but at least one of the above MUST be set to true. The element <ResponseFormat> of the <Usage> MUST be used to indicate the OTP length, the value format and optionally if a check digit is being used. If the use is challenge-response then the <ChallengeFormat> of the <Usage> MUST be used to indicate the challenge minimum and maximum length, its format and optionally if a check digit is being used.

For the <Data> elements of a key of this algorithm, the following subelements MUST be present in either the <Key> element itself or an commonly shared <KeyProperties> element.

* Counter

The following additional constraints apply:

- The value of the <Secret> element MUST contain key material with a length of at least 8 octets (56 bits + parity) if it is present.

- The <ResponseFormat> element MUST have the 'Format' attribute set to "DECIMAL" or "HEXADECIMAL", and the 'Length' attribute

MUST be between 6 and 16.

- The <PINPolicy> element MAY be present but the <Format> child element of the <PINPolicy> element cannot be set to "Algorithmic".

An example of a <Key> of this algorithm is as follows.

```
<?xml version="1.0" encoding="UTF-8"?>
<KeyContainer Version="1.0"
  xmlns="urn:ietf:params:xml:ns:keyprov:pskc:1.0">
    <Device>
        <DeviceInfo>
            <Manufacturer>ActivIdentity</Manufacturer>
            <SerialNo>34567890</SerialNo>
        </DeviceInfo>
        <Key KeyAlgorithm="http://www.actividentity.com/
        2008/04/algorithms/algorithms#ActivIdentity-EVENT"
        KeyId="12345677">
            <Issuer>Issuer</Issuer>
            <Usage OTP="true">
                <ResponseFormat Length="8" Format="DECIMAL"/>
            </Usage>
            <Data>
                <Secret>
                    <PlainValue>
                    MTIzNDU2Nzg5MDEyMzQ1Njc4OTA=
                    </PlainValue>
                </Secret>
                <Counter>
                    <PlainValue>0</PlainValue>
                </Counter>
            </Data>
        </Key>
```

```
    </Device>
  </KeyContainer>
```


12. Security Considerations

[Editor's Note: Security considerations regarding the algorithms go in here.]

13. IANA Considerations

[Editor's Note: The registration of the algorithm profiles goes in here.]

14. Acknowledgements

Add your name here.

15. Normative References

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Authors' Addresses

Philip Hoyer
ActivIdentity, Inc.
117 Waterloo Road
London, SE1 8UL
UK

Phone: +44 (0) 20 7744 6455
Email: Philip.Hoyer@actividentity.com

Mingliang Pei
VeriSign, Inc.
487 E. Middlefield Road
Mountain View, CA 94043
USA

Phone: +1 650 426 5173
Email: mpei@verisign.com

Salah Machani
Diversinet, Inc.
2225 Sheppard Avenue East
Suite 1801
Toronto, Ontario M2J 5C2
Canada

Phone: +1 416 756 2324 Ext. 321
Email: smachani@diversinet.com

Andrea Doherty
RSA, The Security Division of EMC
174 Middlesex Tpk.
Bedford, MA 01730
USA

Email: adoherty@rsa.com