S/MIME Working Group
Internet Draft
Expires: December 2006

G. Appenzeller
Voltage Security
June 2006

Identity-based Encryption Parameter and Policy Lookup

<draft-ietf-smime-ibepps-00.txt>

Status of this Document

Abstract

This document describes a protocol to obtain public parameters and policy information for an identity-based encryption system.

Table of Contents

1. Introduction

An identity-based encryption system (IBE) allows the encryption of messages using a user s identity plus a set of public parameters. Theses public parameters are a global piece of data that is generated together with the master secret of the IBE system when the IBE system is set up. This document defines a protocol to retrieve public parameters as well as configuration parameters of the private key generator (PKG) of an IBE system.

This document does not describe the actual algorithms used for encryption or the mathematical structure of the public parameters, they are described in [IBCS]. It also does not describe the communication protocol to the PKG, which is described in [IBEPKG].

1.1. 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 RFC-2119 [KEY].

2. Overview

For an identity-based encryption (IBE) system to operate correctly, the sender, receiver and the private key generator (PKG) have to agree on a number of parameters. This protocol specifies how a system component of an IBE system can retrieve these parameters, specifically:

1. The Public Parameters of the PKG. The public parameters are part of the encryption (and in some cases decryption) operation of the IBE system. Generation of public parameters and the master secret, as well as the mathematical structure of the public parameters for the BF and BB1 algorithms are described in [IBCS].

2. The URI of the PKG. Knowledge of this URI allows recipients to request a private key as described in [IBEPKG].

3. The schema to format the identity strings. When issuing a private key, the PKG often wants to limit who can obtain private keys. For example for an identity string that contains bob@example.com , only the owner of the identity string should be able to request the private key. To ensure that the PKG can interpret the identity string for which a private key is requested, the encryption engine and the PKG have to use the same schema for identity strings. Identity schemas are described in [IBECMS]

A sending or receiving client MUST allow configuration of these parameters manually, e.g. through editing a configuration file.

However for simplified configuration a client MAY also implement the PP URI request method described in this document to fetch the system parameters based on a configured URI. This is especially useful for federating between IBE systems. By specifying a single URL a client can be configured to fetch all the relevant parameters for a remote PKG. These public parameters can then be used to encrypt messages to recipients who authenticate to and retrieve private keys from that PKG.

Section 3 of this document outlines the URI request method to retrieve a parameter block based on a URI. Section 4 describes the schema of the parameter block itself.

3. Request Method

The configuration URI SHOULD be an HTTPS URL [RFC2616] of the format:

```
http_URL = "https:" "//" host [ ":" port ] [ abs_path ]
```

An example URL for ibe system parameters is

```
https://ibe-0000.example.com/example.com.pem
```

To retrieve the IBE system parameters, the client SHOULD use the HTTP GET method as defined in [RFC2616]. The request SHOULD happen over a secure protocol. The requesting client MUST support either SSL v 3.0 [SSL3] protocol or TLS v 1.1 [TLS]. When requesting the URL the client MUST only accept the system parameter block if the server identity was verified successfully by SSL or TLS [RFC2618].

A successful GET request returns in its body the DER and Base64 encoded ASN.1 structure that is described in the next section.

4. Parameter and Policy Format

The IBE System parameters are a set of

```
IBESysParams ::= SEQUENCE {
   version              INTEGER,
   districtName         UTF8String,
   districtSerial       INTEGER,
   validity             Validity,
   ibePublicParameters  IBEPublicParameters,
   ibeIdentitySchema    OBJECT IDENTIFIER,
   ibeParamExtensions   IBEParamExtensions
}
```

The version specifies the version of the parameter format. For the format described in this standard it MUST be set to 2 The district name is a UTF8String that MUST be a valid domain name as defined by [RFC1035]. The districtSerial is a serial number. If new parameters are published for a district, it MUST be increased.

The Validity is identical to the Validity definition for an X.509 certificate:

```
Validity ::= SEQUENCE {
    notBefore     CertificateValidityDate,
    notAfter      CertificateValidityDate
}

CertificateValidityDate ::= CHOICE {
    utcTime       UTCTime,
    generalTime   GeneralizedTime
}
```

A client SHOULD verify if system parameters that it obtains are currently valid and SHOULD not use these parameters if they are not valid.

IBEPublicParameters is a set of public parameters that correspond to encryption algorithms that the PKG associated with this district understands.

```
IBEPublicParameters ::= SEQUENCE OF IBEPublicParameter

IBEPublicParameter  ::= SEQUENCE {
      ibeAlgorithm         OBJECT IDENTIFIER,
      publicParameterData  OCTET STRING
}
```

The ibeAlgorithm OID specifies an IBE algorithm. The publicParameterData is a DER encoded ASN.1 structure that contains the actual cryptographic parameters. Its specific structure depends on the algorithm. The OIDs for two IBE algorithms, the Boneh-Franklin and Boneh-Boyen algorithms and their publicParameterData structures are defined in [IBCS].

The IBESysParams of a district MUST contain at least one algorithm and MAY contain several algorithms. It MUST NOT contain two or more IBEPublicParameter entries with the same algorithm. A client that wants to use IBESysParams can chose any of the algorithms specified in the publicParameterData structure. If a client does not support any of the supported algorithms it MUST generate an error message.A client MUST implement at least the Boneh-Franklin algorithm and MAY implement the Boneh-Boyens and other algorithms.

ibeIdentitySchema is an OID that defines the type of identities that are used with this district. The OIDs and the required and optional fields for each OID are described in [IBECMS].

IBEParamExtensions is a set of extensions that are defined the same way as X.509 extensions.

```
IBEParamExtensions ::= SEQUENCE OF Extensions

Extension  ::=  SEQUENCE  {
  id         OBJECT IDENTIFIER,
  critical   BOOLEAN DEFAULT FALSE,
  value      OCTET STRING
}

ibeParamExt OBJECT IDENTIFIER ::= {
  ibcs ibcs3(3) parameter-extensions(2)
}
```

The contents of the octet string are defined by the specific extension type. The System Parameters of a district MAY have any number of extensions, including zero. A client that encounters an

extension SHOULD fail if the extension is critical and SHOULD ignore it silently if the extension is not critical.

The Extension pkgURL as defined in section 5 defines the URL of the Private Key Generator of the district. If the PKG is publicly accessible, this extension SHOULD be present to allow the automatic retrieval of private keys for recipients of encrypted messages. For this extension the OCTET STRING contains a UTF8String with the full URL of the key server.

5. ASN.1 Module

This section defines the ASN.1 module for the encodings discussed in section 4.

```
IBEPP { joint-iso-itu(2) country(16) us(840) organization(1)
   identicrypt(114334) ibcs(1) pps(4) version(1) }

DEFINITIONS IMPLICIT TAGS ::= BEGIN

IMPORTS IBEIdentitySchema
  FROM BFCMS
      { joint-iso-itu(2) country(16) us(840) organization(1)
        identicrypt(114334) ibcs(1) cms(4) module(5) version(1)
      };

ibcs OBJECT IDENTIFIER ::= {
   joint-iso-itu(2) country(16) us(840) organization(1)
      identicrypt(114334) ibcs(1)
}

-- The IBE System parameters consist of a set of public parameters
-- for the encryption algorithms supported by the district,
-- the identity schema, the URL of the PKG and further optional
-- parameters

IBESysParams ::= SEQUENCE {
   version              INTEGER,
   districtName         UTF8String,
   districtSerial       INTEGER,
   validity             Validity,
   ibePublicParameters  IBEPublicParameters,
   ibeIdentitySchema    OBJECT IDENTIFIER,
   ibeParamExtensions   IBEParamExtensions
}

-- Validity designates the time interval for which these parameters
-- are valid. It is defined the same as in X.509

Validity ::= SEQUENCE {
    notBefore     CertificateValidityDate,
    notAfter      CertificateValidityDate
}

CertificateValidityDate ::= CHOICE {
    utcTime       UTCTime,
    generalTime   GeneralizedTime
```

```
}

-- Public Parameters for the IBE Algorithm
--   ibeAlgorithm is the algorithm OID from IBCS, e.g. "bb" or "bf"
--   publicParameterData is a DER encoded ASN.1 public parameter
--   block, e.g. BFPublicParamaters, BBPublicParamaters

IBEPublicParameters ::= SEQUENCE OF IBEPublicParameter

IBEPublicParameter  ::= SEQUENCE {
      ibeAlgorithm         OBJECT IDENTIFIER,
      publicParameterData  OCTET STRING
}

-- Extensions are defined the same as in X.509

IBEParamExtensions ::= SEQUENCE OF Extension

Extension  ::=  SEQUENCE  {
  id         OBJECT IDENTIFIER,
  critical   BOOLEAN DEFAULT FALSE,
  value      OCTET STRING
}

ibeParamExt OBJECT IDENTIFIER ::= {
  ibcs ibcs3(3) parameter-extensions(2)
}

-- Defined Extensions:
-- pkgURL:        URL of the PKG, value is a UTF8String

pkgURL        OBJECT IDENTIFIER ::= { ibeParamExt pkgURL(1) }

END
```

6. Security Considerations

This entire document relates to security considerations.

7. IANA Considerations

No further action by the IANA is necessary for the protocols described in this document.

8. References

8.1. Normative References

[CMS] R. Housley, Cryptographic Message Syntax, RFC 3369, August 2002.

[KEY] S. Brander, Key Words for Use in RFCs to Indicate Requirement Levels, BCP 14, RFC 2119, March 1997.

[P1363] IEEE P1363.3, Standards Specifications for Public-Key Cryptography, 2001.

[SSL3] A. Frier, P. Karlton, and P. Kocher, "The SSL 3.0 Protocol", Netscape Communications Corp., Nov 18, 1996.

[TLS] T. Dierks, E. Rescorla, The Transport Layer Security Protocol Version 1.1, RFC 4346, April 2006.

[X509] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.

[IBEARCH] L. Martin, M. Schertler, Identity-based Encryption Architecture, draft-ietf-smime-ibearch-00.txt.

[IBCS] X. Boyen, L. Martin, Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems, draft-ietf-smime-ibcs-00.txt.

[IBECMS] M. Schertler, L. Martin, Using the Boneh-Franklin identity-based encryption algorithm with the Cryptographic Message Syntax (CMS), draft-ietf-smime-bfibecms-01.txt.

[IBEPKG] G. Appezeller Private Key Request protocol for Identity-Based Encryption, draft-ietf-smime-ibepkg-00.txt.

[RFC2396] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.Author's Address

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frysyk, H., Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

Author's Address

Guido Appenzeller
Voltage Security
1070 Arastradero Rd Suite 100
Palo Alto CA 94304

Phone: +1 650 543 1280
Email: guido@voltage.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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