Software Agent Certificate Policy

Draft

Version 0.2.

Milan Sova

Software Agent Certificate Policy: Draft

Version 0.2.
Milan Sova

Table of Contents

1. Introduction

1.1. Overview

This document describes set of provisions which MUST be met by a conforming CA when issuing certificates for software agents.

In this document, the term “software agent” is used to describe any piece of software using for its operation a public key certificate to authenticate itself or for decrypting data in a manner similar to that in which personal certificates are used by persons. Relying parties MAY check the presence of this policy OID in the `policyIdentifier` field of the `certificatePolicies` certificate extension to distinguish between certificates issued to real persons form those issued to software agents.

This policy is intended to be used concurrently with other “general-scope” policies describing provisions not dealt with in this document.

This document is structured according to RFC 3647. Sections irrelevant to the scope of this policy are kept for compatibility. These sections are marked with the “No stipulation.” phrase. Provisions not stipulated by this policy MAY be defined by other policies applied by a conforming CA.

Within this document the words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, “OPTIONAL” are to be interpreted as in RFC 2119. (See Appendix A).

1.2. Document name and identification

1.2.1. Document name

SWAgent1SCertificatePolicy0.2

1.2.2. Object identifier

This policy is identified by the following unique registered Object Identifier (OID):

To be supplied.

1.3. PKI participants

No stipulation.

1.4. Certificate usage

No stipulation.

1.5. Policy administration

1.5.1. Organization administering the document

This policy is maintained by EUGridPMA.

Fill in the addresses.

1.5.2. Contact person

To be supplied.

1.5.3. Person determining CPS suitability for the policy

Suitability of any CPS for this policy is determined by EUGridPMA.

1.5.4. CPS approval procedures

When approving CPS suitability for this policy, EUGridPMA follows procedures defined in its accreditation procedures document EGPMA AP.

1.6. Definitions and acronyms

Certification Authority (CA)	An authority trusted by one or more users to create and assign public key certificates. Optionally the CA may create the user's keys. It is important to note that the CA is responsible for the public key certificates during their whole lifetime, not just for issuing them.
Certificate policy	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.
Certificate subject	The entity (person, organization, or server) whose public key is certified in the certificate.
Certification Practice Statement	A statement of the practices which a certification authority employs in issuing certificates.
Conforming CA	a certificate authority (CA) whose behavior is conforming to the set of provisions specified in this document.
End entity	A person or resource that needs to have their public key certified.
Public Key Certificate	A data structure containing the public key of an end entity and some other information, which is digitally signed with the private key of the CA which issued it.
Registration authority	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).
Relying party	A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. In this document, the terms “certificate user” and “relying party” are used interchangeably.
Subscriber	In the case of certificates issued to resources (such as web servers), the person responsible for the certificate for that resource. For certificates issued to individuals, same as certificate subject.
Software agent	a software application using a public key certificate for authentication or data decryption in a manner similar to that in which personal certificates are used.

2. Publication and repository responsibilities

No stipulation.

3. Identification and authentication

No stipulation.

4. Certificate life-cycle operational requirements

4.1. Certificate Application

No stipulation.

4.2. Certificate application processing

No stipulation.

4.3. Certificate issuance

No stipulation.

4.4. Certificate acceptance

No stipulation.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

No stipulation.

4.5.2. Relying party public key and certificate usage

Relying parties SHOULD recognize subjects of certificates issued under this policy to be software agents and rely on them in an appropriate manner.

4.6. Certificate renewal

No stipulation.

4.7. Certificate re-key

No stipulation.

4.8. Certificate modification

No stipulation.

4.9. Certificate revocation and suspension

No stipulation.

4.10. Certificate status services

No stipulation.

4.11. End of subscription

No stipulation.

4.12. Key escrow and recovery

No stipulation.

5. Facility, management, and operational controls

No stipulation.

6. Technical security controls

6.1. Key pair generation and installation

No stipulation.

6.2. Private key protection and cryptographic module engineering controls

6.2.1. Cryptographic module standards and controls

No stipulation.

6.2.2. Private key (n out of m) multi-person control

No stipulation.

6.2.3. Private key escrow

No stipulation.

6.2.4. Private key backup

No stipulation.

6.2.5. Private key archival

No stipulation.

6.2.6. Private key transfer into or from a cryptographic module

No stipulation.

6.2.7. Private key storage on cryptographic module

The software agents' private key MAY be stored in an unencrypted file to ease its usage. All precautions MUST be taken to prevent the file from unauthorized access.

6.2.8. Method of activating private key

No stipulation.

6.2.9. Method of deactivating private key

No stipulation.

6.2.10. Method of destroying private key

No stipulation.

6.2.11. Cryptographic module rating

No stipulation.

6.3. Other aspects of key pair management

No stipulation.

6.4. Activation data

No stipulation.

6.5. Computer security controls

No stipulation.

6.6. Life cycle technical controls

No stipulation.

6.7. Network security controls

No stipulation.

6.8. Timestamping

No stipulation.

7. Certificate, CRL, and OCSP profiles

7.1. Certificate Profile

7.1.1. Version number(s)

The `version` field in the certificate MUST state 2, indicating X.509v3 certificates.

7.1.2. Certificate extensions

The certificate MUST include `certificatePolicies` extension containing this policy OID in the `policyIdentifier` field.

7.1.3. Algorithm object identifiers

No stipulation.

7.1.4. Name forms

No stipulation.

7.1.5. Name constraints

No stipulation.

7.1.6. Certificate policy object identifier

Certificates issued in accordance with this policy MUST contain the following OID in the following OID in the `policyIdentifier` field of the `certificatePolicies` extension:

Supply the OID.

7.1.7. Usage of Policy Constraints extension

No stipulation.

7.1.8. Policy qualifiers syntax and semantics

No stipulation.

7.1.9. Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2. CRL Profile

No stipulation.

7.3. OCSP Profile

No stipulation.

8. Compliance audit and other assessment

No stipulation.

9. Other business and legal matters

9.1. Fees

No stipulation.

9.2. Financial responsibility

No stipulation.

9.3. Confidentiality of business information

No stipulation.

9.4. Privacy of personal information

No stipulation.

9.5. Intellectual property rights

No stipulation.

9.6. Representations and warranties

No stipulation.

9.7. Disclaimers of Warranties

No stipulation.

9.8. Limitations of Liability

No stipulation.

9.9. Indemnities

No stipulation.

9.10. Term and Termination

No stipulation.

9.11. Individual notices and communications with participants

No stipulation.

9.12. Amendments

9.12.1. Procedure for amendment

Amendments to this policy MUST undergo the same procedures as for the initial approval (see Section 1.5.4). Rephrasing provisions to improve their understandability as well as pure spelling corrections are not considered amendments.

9.12.2. Notification mechanism and period

The amended document SHALL be published on the EUGridPMA document repository before it becomes effective.

9.12.3. Circumstances under which OID must be changed

Substantial changes SHALL cause the OID to be changed. The decision is made by EUGridPMA.

9.13. Dispute resolution procedures

Disputes arising out of this CP SHALL be resolved by the EUGridPMA.

9.14. Governing law

???

9.15. Compliance with applicable law

No stipulation.

9.16. Miscellaneous provisions

9.16.1. Entire agreement

No stipulation.

9.16.2. Assignment

No stipulation.

9.16.3. Severability

Should a clause of this document become void because it is conlficting with the governing law (see Section 9.14) or because it has been declared invalid or unenforceable by a court or other law-enforcing entity, this clause shall become void (and should be replaced as soon as possible by a conforming clause), but the remainder of this document shall remain in force.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5. Force Majeure

No stipulation.

9.17. Other provisions

No stipulation.

References

[RFC 2119] *Key words for use in RFCs to Indicate Requirement Levels*. S. Bradner. RFC 2119. March 1997.

[RFC 3647] *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.* S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. RFC 3647. November 2003.

[EGPMA AP] *Accreditation Procedures*. EU Policy management Authority for Grid Authentication in e-Science. April 2004.

Appendix A. Key words for use in RFCs to Indicate Requirement Levels

According to RFC 2119 Key words for use in RFCs to Indicate Requirement Levels , we specify how the main keywords used in RFCs should be interpreted:

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.

1. **MUST.** This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2. **MUST NOT.** This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

3. **SHOULD.** This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. **SHOULD NOT.** This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

5. **MAY.** This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)