NOKIA

NOKIA CERTIFICATE POLICY FOR NOKIA APPLICATIONS

Document Number: DCT 00205-EN
Date: June 2001

Copyright

Limitation of Liability

Under no circumstances shall Nokia be responsible for any special, incidental, consequential or indirect damages, including but not limited to loss of data or income, howsoever caused, and whether or not Nokia was advised of the possibility of such damages.

Warranty Disclaimer

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, title or non-infringement are made in relation to the accuracy, reliability or contents of this document.

NOKIA

Table of Contents

1 Introduction 4

1.1 Important Note For Relying Parties 4
1.2 Policy identification 4

2 Policy outline 5

3 Certificate Policy provisions 6

3.1 Community and applicability 6
3.2 Rights and Obligations 6
3.3 Liability Disclaimer 6
3.4 Interpretation and Enforcement 7
3.5 Publication and Repository 7

4 Identification and authentication 8

4.1 Initial registration 8

5 Operational Requirements 9

5.1 Technical Security Controls 9
5.2 Certificate profile 9
5.3 CRL profile 10

NOKIA

1 Introduction

1.1 Important Note For Relying Parties

Before using/trusting the certificate(s) related to this Certificate Policy, please ensure you have read and understood the provisions of this document.

1.2 Policy identification

Policy Name	Certificate Policy for Nokia Applications
Policy qualifier	Certificates issued using this policy are only to be used for signing code exchanges by Nokia. They are not to be used for any other structure or purpose and no liability will be accepted for any misappropriation or misuse.
Policy version	1.0
Policy status	Approved
Policy reference/OID (Object Identifier)	1.3.6.1.4.1.94.1.49.1.1.1.1
Date of issue	14 June 2001
Date of expiry	Not applicable.
Related CPS	Nokia PKI CPS version 1

For more information about this Certificate Policy, follow the Nokia Contact Information link from http://www.nokia.com

2 Policy outline

Certificates created under this policy are only to be used for signing software packages created internally by Nokia. They are not valid for any other purpose.

The registration process and creation of the private keys is carried out in a secure environment and fully audited before being despatched to the hosting site for signing by the Nokia Code Signing Root Certification Authority.

The procedure for registration and creation of private keys is documented and available upon request from Nokia.

3 Certificate Policy provisions

3.1 Community and applicability

This Certificate Policy is only valid for signing internally created software using the tools provided by Nokia. The software may be either for internal testing only or for external release. All software to be signed must have been developed according to the Nokia Software Engineering Process (SWEP). Certificates under this policy are not available for any other purpose. They must not be used for signing software which has been personally developed (i.e. non-Nokia) even if developed at Nokia premises and during working hours if done outside of SWEP, or software from any other source.

The service provided by the Certificate Policy is to give the utmost assurance to end-users that the software signed by these certificates has been produced and signed in accordance with defined, secure and fully audited procedures adopted by Nokia to warrant the integrity of the software. The Key usage fields specified within this policy are in accordance with this requirement.

3.2 Rights and Obligations

Nokia's obligation is to ensure that the private key is protected at all times against loss, disclosure, modification or unauthorised use as detailed within this document.

To this end, internal procedures, and auditing, have been introduced. These procedures detail how certificate requests are generated and how the certificates are to be used. The obligation is firmly with Nokia to ensure that the procedures are followed in every case.

Nokia is obligated to inform the Certification Authority immediately if it suspects at any time that the private key has been compromised.

Relying parties are expected to use reasonable judgement before deciding to rely on a certificate based service. If they have any doubt of the validity of the Certificate issued under this policy or of the integrity and secrecy of the corresponding signature keys, they are obliged to, in the first instance, contact Nokia.

3.3 Liability Disclaimer

The Certification Authority and Nokia assume no liability in relation to the use of Nokia Application certificates or associated public / private key pairs.

The Certification Authority, Nokia, or Nokia's employees, make no representations or warranties, express or implied, other than as expressly stated in this Certificate Policy. NO IMPLIED WARRANTY OF ANY KIND, INCLUDING BUT NOT LIMITED TO WARRANTIES OF TITLE OR NON-INFRINGEMENT, OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE BY NOKIA.

In no event shall the Certification Authority or Nokia be liable for any indirect, incidental, special, punitive or consequential damages including but not limited to lost profits, revenues or data even if the Certification Authority or Nokia or both have been advised on the possibility of such damages.

Some jurisdictions may not allow exclusion of certain warranties or limitations of liability. The liability of the Certification Authority or Nokia in such case shall be limited to the greatest extent permitted by applicable laws.

3.4 Interpretation and Enforcement

This Certificate Policy shall be subject to and interpreted according to Finnish law.

3.5 Publication and Repository

There is no publication of certificates or certificate revocation lists (CRLs) associated with this Certificate Policy. In the event of any query or validation check, it will be necessary to contact Nokia directly.

For more information about this Certificate Policy, follow the Nokia Contact Information link from http://www.nokia.com

Information on the repository for the associated CPS and CP can be found at http://www.nokia.com/phones/9210/legal.html

4 Identification and authentication

4.1 Initial registration

Registration will be carried out in accordance with the procedure laid down and documented. This document is available upon request from Nokia.

5 Operational Requirements

Certificates under this policy will only be issued at the specific request of Nokia.
No other certificate applications will be accepted under this policy.

Certificates under this policy will be revoked in cases of;

- Compromise
- Loss of keys
- Change of circumstance rendering certificate invalid.

Certificates will not be subject to suspension under this policy, only revocation.

Valid certificates will automatically be renewed one month before expiry.

5.1 Technical Security Controls

The key pairs are only generated on a specified computer. This computer is subsequently sealed until the certificates are required to sign software.

There are no arrangements for any private key backup within this policy.

The private keys are stored on a dedicated computer and held in a safe until required. The computer is sealed. This seal is examined prior to any use of the computer and replaced with a new seal when any operation requiring signing has been completed. Destruction of the keys, should this be necessary, would be by total destruction of the disk.

5.2 Certificate profile

Version	2
Serial Number	Unique Serial numbers are assigned by the CA
Signature Algorithm	SHA-1 with RSA signature
Issuer Distinguished Name	
Country (C)	Not used
Organization (O)	Nokia
Organizational Unit (OU)	Not used
Common Name (CN)	Nokia Code Signing Root CA
Validity	
Not Before	Time of Issue
Not After	5475 days from Time of Issue
Subject	

Country (C)	Not used
Organization (O)	Nokia
Organizational Unit (OU)	Not used
Common Name (CN)	Nokia Content
Subject Public Key Info	1024 RSA

X.509 Extensions

Authority Key Identifier	Not used
Subject Key Identifier	Not used
Key Usage	
Digital Signature	Yes
Non Repudiation	No
Key Encipherment	No
Data Encipherment	No
Key Agreement	No
Key Certificate Signature	No
Extended Key Usage	Code Signing
CRL Signature	No
Certificate Policies	
Policy Identifier	1.3.6.1.4.1.94.1.49.1.1.1.1

5.3 CRL profile

CRLs are not issued under the Certificate Policy. Any query on the validity of a certificate should be addressed in the first instance to Nokia using the contact given in section 3.5 above.