Crayon Group AS Certification Practices Statement
V. 1.1 – 2018-01-01

1.1 CPS Introduction

This statement defines the policies and procedures followed by Crayon Group AS in the issuance of Public Key Certificate credentials.

Crayon Group AS issues certificates to members of its community. This includes Staff and Partners. In addition, Crayon Group AS may issue a modest number of certificates to others who maintain a loose affiliation with the company, but are not officially listed as Staff or Partners.

1.2 NO WARRANTY

Although Crayon Group AS makes its best efforts to ensure that correct credentials are issued only to appropriate members of the community, Crayon Group AS has limited control over how members of the community protect their own credentials. UNDER NO CIRCUMSTANCES IS Crayon Group AS RESPONSIBLE FOR THE CONSEQUENCES TO A RELYING PARTY OF MAKING USE OF CREDENTIALS Crayon Group AS ISSUES. Crayon Group AS OFFERS NO WARRANTY OF ANY KIND AND DISCLAIMS ANY WARRANTY OF MERCHANTABILITY OR OF FITNESS FOR A PARTICULAR PURPOSE. Crayon Group AS CANNOT BE HELD LIABLE FOR ANY DAMAGES OF ANY KIND WHETHER DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL EVEN IF Crayon Group AS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

1.3 CA Private Key Protection

The private key for this CA is maintained in software on a network connected computer.

Three employees have access to this key and are in a position to manage the CA and issue certificates signed by this key.
In addition, some templates are delegated to other users to issue.

1.4 Authentication upon Registration

In general, Crayon Group AS verifies the identity of people it issues certificates to in a way that is considered proper and appropriate. For all personal certificates except email, the person to whom it is issued can only obtain the certificate by personal appearance. A publicly accepted ID must be shown to prove the right identity of the receiver.
Email certificates are automatically issued based on the users Active Directory account. Only the user to whom the certificate is issued can access the private key.

The possession of a certificate issued by this CA implies that at some point Crayon Group AS believed that the possessor was a member of its community. However, the mere possession of a certificate should not be construed by relying parties that possessor has a current association with Crayon Group AS or that possessor my legally bind Crayon Group AS in any form of negotiation.

1.5 Lifetime of Issued Credential

Normally certificates issued to individuals by this CA are valid from the date of one day prior to the date of issuance (to avoid time zone problems) and for one year. Note however that some applications may require, and the CA may choose to issue, certificates that have arbitrarily shorter validity periods. Certificates issued to individuals will not have validity periods longer than two years.

1.6 Revocation

This CA does revoke certificates.

This CA revokes certificates via a Certificate Revocation List. Crayon Group AS will revoke a certificate when informed by the certificate owner that the key associated with the certificate may have been compromised.
As a rule, Crayon Group AS do revoke certificates for people who leave the employment of Crayon Group AS. Certificates issued to Partners or otherwise affiliated persons or companies will be revoked when the company or person no longer have the need to be authenticated.

1.7 Organisation OID

Crayon Group AS is registered with IANA under OID 1.3.6.1.4.1.51474

1.8 End-User Private Key Protection

Crayon Group AS will instruct the End-User to store private keys in a secure way. Either they should be stored on the hard disk of a computer protected by a password or otherwise widely accepted security mechanisms, or they should be stored on a secure device like a password protected memory stick.

1.9 Certificate Profile

The CA shall issue X.509 version 3 certificates or a later version of X.509 certificates if the company approves such use.

The PKI End-Entity software must support the entire base (non-extension) X.509 fields:

Field Name Description
Signature CA signature to authenticate certificate
Issuer Name of CA
Validity Activation and expiry date for certificate
Subject Subscriber's Distinguished Name
Subject Public Key Information Algorithm ID key
Version of X.509 certificate
Serial Number Unique serial number for certificate

1.9.1 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. Certificate extensions used by certificates issued under these Certificate Policies shall conform to the applicable parts of the Crayon Group AS CA - Profile of Base Fields and Extensions Fields of X.509 Certificates and CRLs.

1.9.2 Algorithm Object Identifiers

The CA and End Entities shall only use algorithms approved by the PKI PMA. The CA shall use and End Entities must support the following symmetric algorithms:

Encryption

AES-128, AES-256, 3DES

The crypto period of any one key should not exceed twenty-four hours.

The list of algorithms to be used by all PKI Entities may change without triggering the issuance of a new Certificate Policy or a change in the CP's OID.

In the event of any change in approved algorithms, the CA shall ensure that Subscribers and Designated Certificate Holders are made aware of changes in the list of algorithms approved for use within Crayon Group AS. The CA shall indicate in its CPS the manner in which it will provide such notice of change.

1.9.3 Name Forms

Every DN must be in the form of an X.501 printable string.

1.9.4 Name Constraints

When used, the name constraints extension shall be populated and processed as described in the Crayon Group AS CA - Profile of Base Fields and Extensions Fields of X.509 Certificates and CRLs.

1.9.5 Certificate Policy Object Identifier

The CA shall ensure that the applicable Policy OID or OIDs is or are contained within the certificates it issues.

1.9.6 Usage of Policy Constraints Extension

When used, the policyConstraint extension shall be populated and processed as described in the Crayon Group AS CA - Profile of Base Fields and Extensions Fields of X.509 Certificates and CRLs.

1.9.7 Policy Qualifiers Syntax and Semantics

When used, the policyQualifiers extension shall be populated and processed as described in the Crayon Group AS CA - Profile of Base Fields and Extensions Fields of X.509 Certificates and CRLs.

1.9.8 Processing Semantics for Critical Certificate Extensions Critical extensions, when marked, shall be interpreted as defined in the Crayon Group AS CA - Profile of Base Fields and Extensions Fields of X.509 Certificates and CRLs.

1.9.9 Acknowledgements

Questions about this Certificate Policy or Certification Practices Statement should be directed to Group IT at Crayon Group AS (support@crayon.com).