IEEE SA STANDARDS ASSOCIATION

# CtlSeriesId Tutorial

IEEE 1609 Working Group, d1.1, 2022-06-06

## General

The CtlSeriesId is an identifier specified in IEEE Std 1609.2.1 and used to identify a Certificate Trust List (CTL) series, where each CTL in the series succeeds and updates the information in the previous CTL. A CTL records the list of root Certificate Authority (CA) certificates that are trusted by an SCMS Manager. These root CAs have agreed to follow and enforce the certificate policies and practices of that SCMS Manager. The SCMS Manager also appoints a group of Electors. Each Elector in the group provides a signature on the CTL contents, enabling other participants in the system to trust the CTL.

The CTL also contains information necessary for the perpetuation of future versions of the CTL: the Elector certificates to be used to sign the next CTL in the series, and the "quorum," which is the minimum number of valid Elector signatures on the next CTL that must be known to any participant in the system for that participant to consider that CTL valid.

The CtlSeriesId is an identifier of the CTL series. It is required to be globally unique and so its allocation is managed by the IEEE RA. It appears in the CTL but does not appear in the Elector certificate. This allows a single Elector certificate to be included in multiple CTLs.

The assignee of an CtlSeriesId is known as the SCMS Manager for that CtlSeriesId. An SCMS Manager may be assigned more than one CtlSeriesId and therefore have oversight responsibility for certificates for have responsibility for the CTLs identified by several different CtlSeriesId.

CtlSeriesId was previously known as ElectorGroupId. On June 30, 2022, the registry previously known as 'ElectorGroupId' was renamed 'CtlSeriesId", with all CtlSeriesId assignments carried forward as ElectorGroupId assignments.

## Use of CtlSeriesId in a CTL

A CTL includes:

- the CtlSeriesId;
- the sequence number, which increments by 1 with each new version of the CTL
- The effective date/time of the CTL; i.e., the time (expressed as seconds since the start of an epoch defined in 1609.2) after which this CTL is authoritative;
- the list of approved Elector certificates to be used to sign the next version of the CTL in the sequence; i.e., the CTL with a sequence number whose value is 1 more than the current sequence number value;
- the list of approved Root CA certificates;
- the quorum; i.e., the number of valid signatures from distinct Electors that must be generated on the next version of the CTL in the sequence for that next CTL version to be valid;
- the signatures of the Electors on the information above; these signatures must be generated by the Electors identified in the trusted Elector list in the previous version of the CTL and must be at least the number given in the quorum field of the previous version of the CTL.

Certificates have their permissions indicated by the Provider Service Identifier (PSID); see the IEEE RA tutorial linked from https://standards.ieee.org/products-services/regauth/psid/index.html for a description of PSID. An Elector certificate contains a PSID for Security Management, with value 0x23, and a Service Specific Permissions field indicating ElectorSsp, as specified in IEEE Std 1609.2.1. This combination indicates that the certificate is an Elector certificate; i.e., that it is entitled to sign CTLs. The CtlSeriesId appears in the CTL but does not appear in the Elector certificate. This allows a single Elector certificate to sign multiple CTLs, so that an Elector could act as a notary service for multiple different SCMS Managers, notarizing that they have made the trust decisions indicated in their CTLs.

As noted above, an SCMS Manager may maintain multiple different CTLs, each with a unique CtlSeriesId. An Elector may serve as signatory for multiple CTLs, some of which may be supported by the same SCMS Manager.

The IEEE RA's Public Listing of CtlSeriesId assignments includes the designated domain of applicability intended by each assigned SCMS Manager. This domain may be specified by combination of region, application, or other characteristic.

## Requirements for CtlSeriesId

The fundamental requirement for the CtlSeriesId is that it is globally unique. The IEEE RA will issue CtlSeriesId values with this requirement in mind.

The IEEE RA may follow policies in allocating CtlSeriesId values that provide structure to the 8-byte CtlSeriesId value.

## Possible Future Developments

At some point in the future, a regulatory authority may establish an SCMS Manager for a group of applications in a region. For example, in the European Union, although the exact mechanisms used differ from those specified in IEEE Std 1609.2.1, a Trust List Manager, analogous to an SCMS manager, has been established by an action of the European Commission. In such a case, the IEEE RA may allocate CtlSeriesId values that are in some way linked to an identifier value for this region.

At some point in the future, national, regional, or supranational organizations may establish a role in allocating CtlSeriesId values for use in their regions of authority. This could lead to a delegated CtlSeriesId registry structure, in which the IEEE RA would delegate authority to allocate a set of CtlSeriesId values, possibly identified by a common set of bits , to a regional authority.

National or supranational regulatory authorities that establish an SCMS Manager may prefer that the IEEE RA treats SCMS Managers associated with a regulatory authority differently from SCMS Managers associated with a private organization. As with the previous two ideas discussed around structuring the management of CtlSeriesId, this idea is something that the IEEE RA is aware of but does not have a formal mechanism to address, as it is currently only a hypothetical concept. If a more formal approach is put in place to distinguish between the standings of different SCMS Managers, this tutorial will be updated to address them.

Details regarding these possible future developments may be documented in future revisions of this tutorial.

## Applying for an CtlSeriesId

To apply for an CtlSeriesId, an applicant provides information indicating an intention to act as an SCMS Manager for an CtlSeriesId.

An assignee of an CtlSeriesId value may apply for additional values, providing a rationale for the need for distinct values. The IEEE RA may respond by requesting further information to establish that there is in fact a need for distinct values.

The CtlSeriesId value is assigned by the IEEE RA at its discretion. An application may request a particular value, or a particular prefix, but the IEEE RA makes no commitment to assign a value consistent with the request.