Kennisnet

Servicebeschrijvingen ECK-ID

SchoolID Services

Inhoud

Document informatie

Status

Auteur	Kennisnet, Marc Fleischeuers
Versie	0.91
Versiedatum	april 2016
Status	Concept

Versiehistorie

Versie	Datum	Auteur	Beschrijving
0.9	6 april 2016	Marc Fleischeuers	Assembled from project service descriptions
0.91	18 april 2016	Marc Fleischeuers	Naar aanleiding van KAT Edu-K overleg

Betrokken/geraadpleegd

Betrokken	Rol

Distributie en goedkeuring

Versie	Datum	Persoon	Goedgekeurd (indien van toepassing)

1. Samenvatting

2. Services

2.1. Create ECK ID

SERVICE DESCRIPTION	**retrieveEckId**
CONTEXT	This service is called by allowed LAS systems to obtain a ECK ID for, for instance, a just enrolled student. This function is called during the process of enrollment, and its availability is business critical.
INPUT	• hpgn: HPgn, oblig, hashed PGN; • chainID: xsd:string, oblig, Identifier for ECK chain • sectorID: xsd:string, oblig, Identifier for educational sector
VALIDATIONS	• The calling system, identified by its OIN in the SerialNumber field of the Certificate, is checked against the list of allowed callers (NotAllowedCallerException on failure) • The calling school is identified from the OIN in the wsa:from SOAP header. If the school is not in the list of allowed schools, a NotAllowedCallerException will be thrown • hashed PGN, SectorID, ChainID: format validations (Format Exception specific for argument on failure, e.g. InvalidHPgnException, InvalidChainIdException and InvalidSectorIdException). • SectorID is one of the IDs of educational sectors (InvalidSectorIdException on failure). • ChainID is one of the IDs in chains (InvalidChainIdException on failure) • Hashed PGN is not in substitutionList.old (BlockedHPgnException on failure)
OPERATION	The service combines the three inputs and from the result derives a valid ECK ID. The derivation of a valid ECK ID is performed by a component that is specified in software configuration. If the provided hashed PGN is in substitutionList.new and sectorID is equal to the substitutionlist.sectorID and today is later than substitutiontable.effectivedate, the previous hashed PGN is used to derive the ECK ID from.
OUTPUT	eckID: EckID, The derived ECK ID
EXCEPTIONS	• Format Exception (includes information on which format failed) • InvalidSectorIdException InvalidChainIdException InvalidHPgnException • BlockedHPgnException • NotAllowedCallerException • HashOperationException • TemporaryBlockedException • AbstractNummervoorzieningException
REMARKS	• hpgn is created using scrypt with the prescribed parameters. See the developer documentation on the wiki[1]. • chainID, sectorID are in the form of OBK URN's. Retrieve these values using the retrieveChains, retrieveSectors operations respectively. • eckID is in the form of a URL: https://id.school/2015-09/[128-char hex string]. Currently this url resolves to a static page containing general information about the ECK ID.

2.2. Change ECK ID (subsitution)

SERVICE DESCRIPTION	**replaceEckId**

[1] https://developers.wiki.kennisnet.nl/index.php?title=Nummervoorziening:Hoofdpagina

CONTEXT	This service is called when a school administration needs to indicate that a student is assigned a new PGN by the authorities. A change of PGN number is handled as follows: the old and the new hashed PGN, the sectorID and chainID are recorded in the database; subsequent requests for the old PGN are rejected, and for requests with the new hashed PGN and the same SectorID, the old hashed PGN is used to derive the ECK ID from. See also service description Create ECK ID.
INPUT	• hpgnOld, hpgnNew: HPgn, oblig, resp. Old hashed PGN and new Hashed PGN • chainID: xsd:string, oblig, Identifier for ECK chain • sectorID: xsd:string, oblig, Identifier for educational sector • effectiveDate: xsd:date, optional, 'now' if not given, date and time that the change should take effect
VALIDATIONS	• The calling system identified by its OIN in the Certificate is checked against the list of allowed callers (NotAllowedCallerException on failure) • The calling school is identified from the OIN in the wsa:from header. If the school is not in the list of allowed schools, a NotAllowedCallerException will be thrown • Format validations on input arguments (format Exception specific for argument on failure). • SectorID is one of the IDs of educational sectors (InvalidSectorIdException on failure). • ChainID is one of the IDs in chains (InvalidChainIdException on failure) • Old hashed pgn is not already in the substitution table (old and new) (InvalidPgnException otherwise) • New hashed pgn is not already in the substitution table (old and new) (InvalidPgnException otherwise) • Effective date: if given, is valid and in the future(xml parse error in case of invalid date format))
OPERATION	Old hashed PGN, new Hashed PGN, chain ID and sectorID are recorded in the substitution table, and a ECK ID for the new hashed PGN is derived using function 'Create ECK ID'.
OUTPUT	eckID: EckId, The derived ECK ID for the new hpgn
EXCEPTIONS	• InvalidSectorIdException • InvalidChainIdException • InvalidPgnException with information on which hashed PGN is invalid, and why • BlockedHPgnException • NotAllowedCallerException • HashOperationException • TemporaryBlockedException • AbstractNummervoorzieningException
REMARKS	• hpgnOld, hpgnNew is created using scrypt with the prescribed parameters. See the developer documentation on the wiki[2]. • chainID, sectorID are in the form of OBK URN's. Retrieve these values using the retrieveChains, retrieveSectors operations respectively. • eckID is in the form of a URL: https://id.school/2015-09/[128-char hex string]. Currently this url resolves to a static page containing info about the ECK ID.

2.3. Batch creation of ECK IDs

SERVICE DESCRIPTION	**submitEckIdBatch**

[2] https://developers.wiki.kennisnet.nl/index.php?title=Nummervoorziening:Hoofdpagina

CONTEXT	This service is called by allowed LAS systems to submit a list of hashed PGNs, for a single Sector and a single Chain. The system processes the list and makes a corresponding list of ECK IDs available for retrieval (see retrieveEckBatch).

INPUT	• hpgnList: a list of 1..20.000[3]
	  ○ int: xsd:int, oblig, sequence number
	  ○ hPgn: HPgn hashed PGNs
	• chainID: xsd:string, oblig, Identifier for ECK chain
	• sectorID: xsd:string, oblig, Identifier for educational sector

VALIDATIONS	• The calling system identified by its OIN in the Certificate is checked against the list of allowed callers (NotAllowedCaller Exception on failure) • The calling school is identified from the OIN in the wsa:from header. If the school is not in the list of allowed schools, a NotAllowedCallerException will be thrown • The system validates the size of the input (TemporaryBannedException if too many hPgns are submitted) • The system validates the frequency of calls (TemporaryBannedException if there are too many calls registered) • SectorID is one of the IDs of educational sectors (InvalidSectorIdException on failure). • ChainID is one of the IDs in chains (InvalidChainIdException on failure) • Hashed PGN is not in substitutionList.old (offending hPgn is added to the failed list for output)
OPERATION	The service creates a ECK ID for each hashed PGN in the input list and adds it to the list of generated ECK IDs for output. If the list does not contain a hashed PGN or if the hashed PGN was previously indicated as changed, no ECK ID will be created and a message to indicate the nature of the failure will be added to the list of failed PGNs for output. If the provided hashed PGN is in substitutionList.new and sectorID is equal to the substitutionlist.sectorID and today is later than substitutiontable.effectivedate, the previous hashed PGN is used to derive the ECK ID from.
OUTPUT	• batchIdentifier: xsd:string, identifier of the batch request. This identifier can be used to obtain the result, using retrieveEckBatch
EXCEPTIONS	• InvalidSectorIdException InvalidChainIdException InvalidHPgnException • BlockedHPgnException • NotAllowedCallerException • HashOperationException • TemporaryBlockedException • AbstractNummervoorzieningException
REMARKS	The use of this service is limited to prevent abuse: • A batch may contain at most 20.000 hashed PGNs • A batch operation may be submitted at most 3 times per 24 hours These limits are configured in the software and can be modified. Schools that exceed these limits are temporarily banned from submitting batch requests. Schools may contact Kennisnet servicedesk for information and for lifting of the bans. Schools may submit multiple batch requests, as long as the limits are observed. Batches are processed in the order in which they occur.

[3] The size of the array is comfigured in software. Actual limit may differ.

	A batch result is available within one hour after submission of the request. Batch results are removed after successful retrieval. The system may remove batch results that are not retrieved within 24 hours.

SERVICE DESCRIPTION	**retrieveEckIdBatch**
CONTEXT	This service is called by allowed LAS systems to retrieve the status and result of a batch request.
INPUT	• batchIdentifier: xsd:string, oblig, the batch identifier obtained in the response from a batch submission (see submitEckIdBatch)
VALIDATIONS	• The calling system identified by its OIN in the Certificate is checked against the list of allowed callers (NotAllowedCallerException on failure) • The calling school is identified from the OIN in the wsa:from header. If the school is not in the list of allowed schools, a NotAllowedCallerException will be thrown • The system validates the frequency of calls (TemporaryBlockedException if there are too many calls registered) • If the batch indicated by the input is purged, already retrieved, or not ready yet, a BatchRetrieveException is returned
OPERATION	The service creates a ECK ID for each hashed PGN in the input list and adds it to the list of generated ECK IDs for output. If the list does not contain a hashed PGN or if the hashed PGN was previously indicated as changed, no ECK ID will be created and a message to indicate the nature of the failure will be added to the list of failed PGNs for output.

OUTPUT	• Success: an optional list of 1..20000[4]:
	  ○ Index: int, the sequence number of the corresponding hPgn from the input
	  ○ EckId: EckId, the ECK ID of the hPgn indicated by the sequence number from the input
	• Failed: an optional list of 1..20000[5]:
	  ○ Index: int, the sequence number of the corresponding hPgn from the input
	  ○ errorMessage: string, indication of the error that occurred when computing the ECK ID

EXCEPTIONS	• InvalidSectorIdException • InvalidChainIdException • InvalidHPgnException • BlockedHPgnException • NotAllowedCallerException • HashOperationException • TemporaryBlockedException • AbstractNummervoorzieningExceptionBatchRetrieveException
REMARKS	The use of this service is limited to prevent abuse: a batch retrieval may be attempted at most once per 15 minutes (software configurable; actual limit may differ). In case this limit is exceeded, the offending school is temporarily banned from using this service. Schools may contact Kennisnet servicedesk for more information and to lift the ban. A batch result is available within one hour after submission of the request. Batch results are removed after successful retrieval. Batch results that are not retrieved can be removed after 24 hours.

[4] Limit is set in in software configuration; actual values may differ
[5] Idem

	In the output of this function, both success and failure are optional arrays. If none of the input fail, the response will contain only 'success' values. If none of the input succeed, the response will contain only 'failure'.

2.4. Retrieving chains and sectors

SERVICE DESCRIPTION	**retrieveChains**
CONTEXT	This service is called by allowed LAS systems to obtain the list of chain parties for which an ECK ID can be derived. As this list changes rarely, this service will not be called often, probably not more than once per day per LAS.
INPUT	none
VALIDATIONS	• The calling system identified by its OIN in the Certificate is checked against the list of allowed callers (NotAllowedCallerException on failure) • The calling school is identified from the OIN in the wsa:from header. If the school is not in the list of allowed schools, a NotAllowedCallerException will be thrown
OPERATION	The service retrieves the list of active Chain Parties
OUTPUT	List of 1 or more : • Id: xsd:string, Identifier of chain that can be used to create ECK IDs for this chain • Name: xsd:string, unique and short name for this chain • Description: xsd:string, human-readable description for this chain • lastEdited: xsd:date, last time this entry was modified
EXCEPTIONS	NotAllowedCallerException
REMARKS	• Currently, only one chain is available in the system, the ECK chain. It's value is http://purl.edustandaard.nl/begrippenkader/e7ec7d3c-c235-4513-bfb6-e54e66854795

SERVICE DESCRIPTION	**retrieveSectors**
CONTEXT	This service is called by allowed LAS systems to obtain the list of school types for which an ECK ID can be derived. As this list changes rarely, this service will not be called often, probably not more than once per day per LAS.
INPUT	none
VALIDATIONS	• The calling system identified by its OIN in the Certificate is checked against the list of allowed callers (NotAllowedCallerException on failure) • The calling school is identified from the OIN in the wsa:from header. If the school is not in the list of allowed schools, a NotAllowedCallerException will be thrown
OPERATION	Retrieve the list of active SectorIDs from the database.
OUTPUT	List of 1 or more : • Id: xsd:string, Identifier of sector that can be used to create ECK IDs for this sector • Name: xsd:string, unique and short name for this sector • Description: xsd:string, human-readable description for this sector • lastEdited: xsd:date, last time this entry was modified
EXCEPTIONS	NotAllowedCallerException
REMARKS	• Currently, thee educational sectors are available in the system:

	○ Primair onderwijs: http://purl.edustandaard.nl/begrippenkader/512e4729-03a4-43a2-95ba-758071d1b725 ○ VO: http://purl.edustandaard.nl/begrippenkader/2a1401e9-c223-493b-9b86-78f6993b1a8d ○ MBO: http://purl.edustandaard.nl/begrippenkader/f3ac3fbb-5eae-49e0-8494-0a44855fff25 The names, descriptions and values are taken from OBK.

2.5. Ping operation

SERVICE DESCRIPTION	**pingRequest**
CONTEXT	This service is called by allowed LAS systems to verify the service is alive.
INPUT	none
VALIDATIONS	• The calling system identified by its OIN in the Certificate is checked against the list of allowed callers (NotAllowedCallerException on failure) • The calling school is identified from the OIN in the wsa:from header. If the school is not in the list of allowed schools, a NotAllowedCallerException will be thrown
OPERATION	Verify the database is available for operation
OUTPUT	• Available: Boolean, the system is available (true) or not (false) • applicationVersion: string, identifier for the implementation version • systemTime: xsd:dateTime, timestamp of the current system time
EXCEPTIONS	NotAllowedCallerException
REMARKS	•

3. Common types

Name	HPgn
Fields	xsd:string
Constraints	• Is not empty • does not exceed length of 128
Remarks	Contains the result of the prescribed hash function SCrypt

Name	EckId
Fields	xsd:string
Constraints	• Is not empty
Remarks	Format is https://id.school/[version]/[128 char hex string]. The version will initially be “2015-09”.

4. Exceptions

Exceptions will be presented by the Nummervoorziening Service as Soap faults. To distinguish the cause Exception of an operation at the client, the element faultactor will hold the specific Exception. In the detail node, a message node is added with additional information regarding the Exception.

Example of a Soap fault as a response from the Nummervoorziening Service (omitting the Soap Headers):

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <soap:Fault>
      <faultcode>soap:SERVER</faultcode>
      <faultstring>RetrieveEckIdBatch has thrown an exception while building the response</faultstring>
      <faultactor>InvalidBatchIdentifierException</faultactor>
      <detail>
        <message>Batch with specified identifier does not exist</message>
      </detail>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

The reference clients will contain code in Java and C# to handle these faults and distinguish root causes.