Kennisnet

# Servicebeschrijvingen ECK-ID

## SchoolID Services

# Inhoud

# Document informatie

## Status

| | |
|---|---|
| Auteur | Kennisnet, Marc Fleischeuers |
| Versie | 1.0.10 |
| Versiedatum | 23 januari 2017 |
| 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 |
| 0.92 | 27 mei 2016 | Marc Fleischeuers | Exceptions in lijn met realisatie; hpgn format; sample SOAP messages |
| 1.0 | 12 juli 2017 | Marc Fleischeuers | |
| 1.0.9 | 23 januari 2017 | Marc Fleischeuers | Wijzigingen wetgeving (introductie stampseudoniem) |
| 1.0.10 | 6 april 2017 | Marc Fleischeuers | Substitutie van stampseudoniem ipv ECK ID |

## Betrokken/geraadpleegd

| Betrokken | Rol |
|---|---|
| | |
| | |

## Distributie en goedkeuring

| Versie | Datum | Goedgekeurd (indien van toepassing) |
|---|---|---|
| 1.0.9 | 21-3-2017 | Tactisch overleg Toegang tot leermateriaal |
| 1.0.10 | | |

# 1. Samenvatting

# 2. Services

## 2.1. Create Stem Pseudonym

| | |
|---|---|
| **SERVICE DESCRIPTION** | **retrieveStempseudonym** |
| **CONTEXT** | This service is called by allowed LAS systems to obtain a stem pseudonym 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; |
| **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)<br>• 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<br>• hashed PGN: format validations (InvalidHPgnException on failure) |
| **OPERATION** | The service derives a stem pseudonym from the input. The derivation of a valid stem pseudonym is performed by a component that is specified in software configuration. |
| **OUTPUT** | stempseudonym: The generated stem pseudonym |
| **EXCEPTIONS** | • NotAllowedCallerException<br>• HashOperationException (indicates server configuration error) |
| **REMARKS** | • |

## 2.2. 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** | • Stempseudonym: Stem pseudonym, obtained with 'retrieveStempseudonym'<br>• chainID: xsd:string, oblig, Identifier for ECK chain<br>• 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)<br>• 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<br>• Stem pseudonym, SectorID, ChainID: format validations (Format Exception specific for argument on failure, e.g. InvalidStemPseudonymException, InvalidChainIdException and InvalidSectorIdException).<br>• SectorID is one of the IDs of educational sectors (InvalidSectorIdException on failure).<br>• ChainID is one of the IDs in chains (InvalidChainIdException on failure)<br>• 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.<br>If the provided stem pseudonymis in substitutionList.new and sectorID is equal to the substitutionlist.sectorID and today is later than substitutiontable.effectivedate, the previous stem pseudonym is used to derive the ECK ID from. |
| **OUTPUT** | eckID: EckID, The derived ECK ID |

| | |
|---|---|
| **EXCEPTIONS** | • InvalidSectorIdException InvalidChainIdException InvalidHPgnException<br>• BlockedStempseudonymException<br>• NotAllowedCallerException<br>• HashOperationException (indicates server configuration error) |
| **REMARKS** | • chainID, sectorID are in the form of OBK URN's. Retrieve these values using the retrieveChains, retrieveSectors operations respectively.<br>• eckID is in the form of a URL: https://id.school/201703/[128-char hex string]. Currently this url resolves to a static page containing general information about the ECK ID. |

## 2.3. Change stem pseudonym (subsitution)

| | |
|---|---|
| **SERVICE DESCRIPTION** | **replaceStempseudonym** |
| **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 stem hashed PGN are recorded in the database; subsequent requests for the old hashed PGN are rejected, and for requests with the new stem hashed PGN, the old hashed PGN is used to derive the stem pseudonym from. See also service description Create stempseudonym. |
| **INPUT** | • hPGNOld, hPGNNew: oblig, resp. previous hashed PGN and new hashed PGN<br>• 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)<br>• 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<br>• Format validations on input arguments (format Exception specific for argument on failure).<br>• Old hPGN is not already in the substitution table (old and new) (BlockedPGNException otherwise)<br>• New hPGN is not already in the substitution table (old and new) (BlockedPGNException otherwise)<br>• Old and new hPGN are different (substitutionOperationException otherwise)<br>• Effective date: if given, is valid and in the future (xml parse error in case of invalid date format) |
| **OPERATION** | Old hPGN, new hPGN are recorded in the substitution table, and a stem pseudonym for the new hPGN is derived using function 'Create stem pseudonym'. |
| **OUTPUT** | stem pseudonym: The stem pseudonym for the new hpgn |
| **EXCEPTIONS** | • InvalidhPGNException with information on which stem pseudonym is invalid, and why<br>• SubstitutionOperationException<br>• NotAllowedCallerException<br>• HashOperationException (indicates server configuration error) |
| **REMARKS** | • Stem pseudonym is in the form of a URL: https://id.school/spv1/[128-char hex string]. |

## 2.4. Batch creation of stem pseudonyms

| | |
|---|---|
| **SERVICE DESCRIPTION** | **submitStempseudonymBatch** |
| **CONTEXT** | This service is called by allowed LAS systems to submit a list of stem pseudonyms, for a single Sector and a single Chain. The system processes the list and makes a |

| | |
|---|---|
| | corresponding list of stem pseudonyms available for retrieval (see retrieveEckBatch). |
| **INPUT** | • stempseudonymList: a list of 1..20.000[1]<br>  ○ int: xsd:int, oblig, sequence number<br>  ○ hPgn: HPgn hashed PGNs |
| **VALIDATIONS** | • The calling system identified by its OIN in the Certificate is checked against the list of allowed callers (NotAllowedCaller Exception on failure)<br>• 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<br>• The system validates the size of the input (TemporaryBannedException if too many hPgns are submitted)<br>• All indexes are unique (DuplicateIndexHPgnListException otherwise) |
| **OPERATION** | The service creates a stem pseudonym for each hashed PGN in the input list and adds it to the list of generated stem pseudonyms for output. If the list does not contain a hashed PGN or if the hashed PGN was previously indicated as changed, no stem pseudnym will be created and a message to indicate the nature of the failure will be added to the list of failed items for output. |
| **OUTPUT** | • batchIdentifier: xsd:string, identifier of the batch request. This identifier can be used to obtain the result, using retrieveEckBatch |
| **EXCEPTIONS** | • InvalidSectorIdException InvalidChainIdException InvalidHPgnException<br>• NotAllowedCallerException<br>• HashOperationException (indicates server configuration error)<br>• DuplicateIndexHPgnListException |
| **REMARKS** | The use of this service is limited to prevent abuse:<br>• A batch may contain at most 20.000 hashed PGNs<br>• A batch operation may be submitted at most 3 times per 24 hours<br><br>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.<br><br>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. |

## 2.5. Batch creation of ECK IDs

| **SERVICE DESCRIPTION** | **submitEckIdBatch** |
|---|---|
| **CONTEXT** | This service is called by allowed LAS systems to submit a list of stem pseudnyms, 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** | • stempseudonymList: a list of 1..20.000[2]<br>  ○ int: xsd:int, oblig, sequence number<br>  ○ stempseudonym: Stem pseudonym<br>• chainID: xsd:string, oblig, Identifier for ECK chain<br>• 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) |

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

| | |
|---|---|
| | • 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<br>• The system validates the size of the input (TemporaryBannedException if too many stem pseudonyms are submitted)<br>• All indexes are unique (DuplicateIndexHPgnListException otherwise)<br>• SectorID is one of the IDs of educational sectors (InvalidSectorIdException on failure).<br>• ChainID is one of the IDs in chains (InvalidChainIdException on failure)<br>• Stempseudonyms is not in substitutionList.old (offending stem pseudonym 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<br>• BlockedHPgnException<br>• NotAllowedCallerException<br>• HashOperationException (indicates server configuration error)<br>• DuplicateIndexHPgnListException |
| **REMARKS** | The use of this service is limited to prevent abuse:<br>• A batch may contain at most 20.000 hashed PGNs<br>• A batch operation may be submitted at most 3 times per 24 hours<br><br>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.<br><br>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)<br>• 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<br>• The system validates the frequency of calls (SchoolTemporaryBlockedException or BatchTemporaryBlockedException if there are too many calls registered)<br>• The batch result can be retrieved at most once; ContentAlreadyRetrievedException is returned if the batch was retrieved earlier |

| | |
|---|---|
| | • If the batch indicated by the input is purged, already retrieved, or not ready yet, a NotFinishedException is returned |
| **OPERATION** | The service retrieves the batch result (either StempseudonymBatch or EckIdBatch), if available, and returns it to the caller. If an error during check or processing occurs, the error is returned. |
| **OUTPUT** | • Success: an optional list of 1..20000[3]:<br>  ○ Index: int, the sequence number of the corresponding entry from the input<br>  ○ EckId: EckId, the ECK ID of the entry indicated by the sequence number from the input<br>• Failed: an optional list of 1..20000[4]:<br>  ○ Index: int, the sequence number of the corresponding entry from the input<br>  ○ errorMessage: string, indication of the error that occurred when computing the ECK ID |
| **EXCEPTIONS** | • InvalidSectorIdException<br>• InvalidChainIdException<br>• InvalidHPgnException<br>• BlockedHPgnException<br>• NotAllowedCallerException<br>• HashOperationException (indicates server configuration error)<br>• SchoolTemporaryBlockedException, BatchTemporaryBlockedException<br>• ContentAlreadyRetrievedException<br>• NotFinishedException<br>• |
| **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.<br><br>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.<br><br>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'. |

## 2.6. 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)<br>• 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 : |

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

| | |
|---|---|
| | • Id: xsd:string, Identifier of chain that can be used to create ECK IDs for this chain<br>• Name: xsd:string, unique and short name for this chain<br>• Description: xsd:string, human-readable description for this chain<br>• 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)<br>• 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 :<br>• Id: xsd:string, Identifier of sector that can be used to create ECK IDs for this sector<br>• Name: xsd:string, unique and short name for this sector<br>• Description: xsd:string, human-readable description for this sector<br>• lastEdited: xsd:date, last time this entry was modified |
| **EXCEPTIONS** | NotAllowedCallerException |
| **REMARKS** | • Currently, thee educational sectors are available in the system:<br>  ○ Primair onderwijs: http://purl.edustandaard.nl/begrippenkader/512e4729-03a4-43a2-95ba-758071d1b725<br>  ○ VO: http://purl.edustandaard.nl/begrippenkader/2a1401e9-c223-493b-9b86-78f6993b1a8d<br>  ○ MBO: http://purl.edustandaard.nl/begrippenkader/f3ac3fbb-5eae-49e0-8494-0a44855fff25<br>The names, descriptions and values are taken from OBK. |

## 2.7. 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)<br>• 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)<br>• applicationVersion: string, identifier for the implementation version<br>• systemTime: xsd:dateTime, timestamp of the current system time |

| | |
|---|---|
| **EXCEPTIONS** | NotAllowedCallerException |
| **REMARKS** | • |

# 3. Sample Messages

New versions of the sample messages will be provided when the new version of the software is available.

# 4. Common types

| | |
|---|---|
| **Name** | HPgn |
| **Fields** | xsd:string |
| **Constraints** | • Consists of 64 hex characters ([0-9][A-Z][[a-z]){64} |
| **Remarks** | Contains the result of the prescribed hash function SCrypt |

| | |
|---|---|
| **Name** | EckId |
| **Fields** | xsd:string |
| **Constraints** | • Is not empty |
| **Remarks** | |

# 5. 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.