Documentation

Nets Rights Management (Attribute Service)

Contents

List of illustrations

Version history

19-12-2008	First draft	KNS
11-11-2011	Updates	PKRIS
02-05-2012	Issuer and WSDL for test og prod added	KNS
11-11-2014	WSDL and Service endpoint, contact information	KMAIB

List of appendices

Appendix 1 Order form

1 Introduction

1.1 What is Attribute Service?

The Attribute Service – also known as Nets Rights Management – makes it possible for companies to assign attributes (roles or rights) to employees with employee certificates.

Attributes are allocated in the administrator's self-service system – the system used to create and administer employee certificates. In practical terms, the administrator locates the employee and links the relevant attributes to the employee's employee certificate. The link is made in a special area of the self-service system.

The service provider defines:

- which attributes should be accessible, and
- which companies (CVR numbers) should be able to see and select the attribute in the self-service system.

Companies are not charged for assigning and using attributes. The service provider pays for the set-up and operation of the Attribute Service.

1.2 Example of using attributes

An employee needs to report pension information to your pension fund on behalf of the company.

The pension fund uses the Attribute Service to make available an attribute called "Pensions notifier", for example. The company's administrator (Local Registration Authority – LRA) assigns this attribute to one of the company's employees by linking the attribute with the particular employee's employee digital signature. When the employee tries to access the pension fund's online service to report pension information using the employee digital signature, the pension fund will be able to verify whether the necessary attribute has been linked to the employee in question. If so, access is granted to report pension information on behalf of the company in question.

Any other employee without this attribute would be rejected by the pension fund.

1.3 Who creates the attributes?

Various companies and public authorities make attributes available to other parties by agreement with Nets DanID.

1.4 Who can use attributes?

Some attributes are only made available to selected CVR numbers, while other attributes are visible and can be selected by any CVR numbers that have employee digital signatures. If the attribute

is visible to the administrator during self service, the company will be able to use it. It is usually possible to link the same attributes to one or more employees.

1.5 Who needs attributes?

The need to use attributes is governed by the services, facilities, etc., that the company's employees need to use. Normally, the service provider (e.g. the pension fund, in the above example) will notify the company that a specific attribute needs to be linked to an employee digital signature in order to be able to use the service.

1.6 Enquiries about attributes

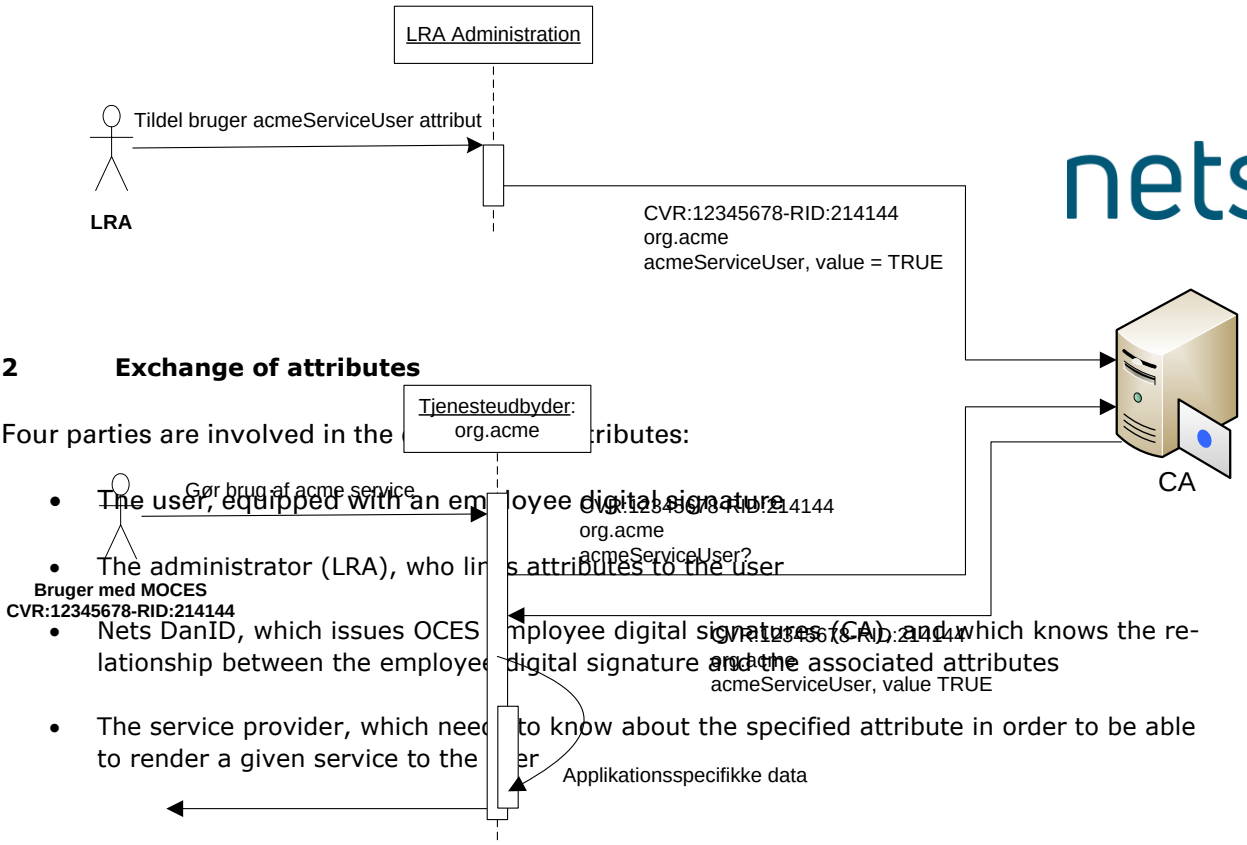
Nets DanID protects a specified attribute (namespace) from delivery to undesirable service providers, as follows:

- An attribute can be available to all service providers for lookup
- An attribute can be available for lookup by the specified service provider in accordance with an agreement between Nets DanID and the attribute owner
- An attribute can be available to all application service providers for verification
- An attribute can be available for verification by the specified service provider in accordance with an agreement between Nets DanID and the attribute owner

1.7 Validation of attribute content

Nets DanID validates attribute syntax, but does not otherwise verify the contents or values of assigned attributes.

It is up to the company/LRA and the service provider to establish the necessary trust in relation to attribute content.



2 Exchange of attributes

Four parties are involved in the [illegible]tributes:

- The user, equipped with an employee digital signature
- The administrator (LRA), who lin[illegible]s attributes to the user
- Nets DanID, which issues OCES employee digital signatures (CA), and which knows the relationship between the employee digital signature and the associated attributes
- The service provider, which need[illegible] to know about the specified attribute in order to be able to render a given service to the [illegible]er

Illustration1: Example of attribute lookup

3 Create/remove attributes

3.1 Who can create/remove attributes?

Nets DanID maintains a "list" of individuals permitted to administer attributes on behalf of the organisation in question. As a rule, the list includes all registered administrators (LRA) for the organisation in question. Additional names can be added at the time of entering into the agreement.

Only someone who is already on the list can add or remove another individual. Notifications concerning this must be e-mailed. The e-mail must be digitally signedusing the employee digital signature of the employee in question.

3.2 Ordering new attributes

The order form available from Nets DanID support must be used to order new attributes.

Nets DanID will contact the requesting party if the attribute is complex and its functionality needs confirming.

3.3 Removing existing attributes

To have existing attributes removed, please e-mail Nets DanID.

4 Attribute web service

The attribute web service is made available to service providers by Nets DanID.

Below is a brief description of the available operations.

4.1 Operations and input parameters

4.1.1 publishAttribute

The *publishAttribute*operation allows a service provider to make an attribute visible to LRAs in a specified company.

Input values: The attribute ID, the company's CVR number.

4.1.2 endPublishAttribute

The *endpublishAttribute* operation allows the service provider to make an attribute invisible to LRAs in a specified company.

Input values: The attribute ID, the company's CVR number.

4.1.3 getAttribute

The *getAttribute* operation allows the service provider to ask for the value of a given attribute for a given employee.

Input: The attribute ID, the subjectSerialNumber of the employee's certificate.

4.1.4 getAttributes

The *getAttributes* operation allows the service provider to undertake multiple *getAttribute* calls in a single call.

Input: list of the input for getAttributes

4.1.5 verifyAttribute

The *verifyAttribute* operation allows the service provider to verify the value of a given attribute for a given employee.

Input: the attribute ID, the attribute value, the subjectSerialNumber of the employee's certificate.

4.2 WSDL

Test environment

WSDL: https://ws-erhverv.pp.certifikat.dk/attributeservice_serviceprovider_server/?WSDL
Service endpoint: https://ws-erhverv.pp.certifikat.dk/attributeservice_serviceprovider_server

Production environment

WSDL: https://ws-erhverv.certifikat.dk/attributeservice_serviceprovider_server/?WSDL
Service endpoint: https://ws-erhverv.certifikat.dk/attributeservice_serviceprovider_server

Issuer is "TRUST 2408"

WS call	Input parameter	Description
publishAttribute	Attribute ID Company CVR number	The *publishAttribute* operation allows a service provider to make an attribute visible to LRAs in a specified company.
endPublishAttribute	Attribute ID Company CVR number	The *endpublishAttribute* operation allows the service provider to make an attribute invisible to LRAs in a specified company.
getAttribute	Attribute ID The subjectSerialNumber of the employee's certificate, e.g. CVR:30808460-RID:1256293651992	The *getAttribute* operation allows the service provider to ask for the value of a given attribute for a given employee.
getAttributes	List of the input for getAttribute	The *getAttributes* operation allows the service provider to undertake multiple *getAttribute* calls in a single call.
verifyAttribute	Attribute ID Attribute value	The *verifyAttribute* operation allows the service provider to verify

	The subjectSerialNumber of the employee's certificate	the value of a given attribute for a given employee.

4.3 Return values

The following self-explanatory return values are supported for each call to the web service:

STATUS_OK = 0
UNKNOWN_ATTRIBUTE = 101
REFERRAL_ATTRIBUTE = 102

LOOKUP_NOT_ALLOWED = 103

VERIFICATION_NOT_ALLOWED = 104
ISSUER_NOT_SUPPORTED = 105
UNKNOWN_USER = 106
ATTRIBUTE_NOT_CONFIGURED_FOR_USER = 107
STATUS_ERROR = 108
VALUE_NOT_VERIFIED = 109

5 Contact information

Nets DanID can be contacted concerning attributes using the web formula: http://www.nets.eu/dk-da/Service/kundeservice/nemid-tu/Pages/Contact-NemID-serviceprovider-support.aspx