

# SAML Profile for Federation in Danish Public Sector V2.0 (DK-SAML 2.0)

Answer to Hearing Document  
Submitted by IT- og Telestyrelsen

---

 September 21. 2007 [www.novell.com](http://www.novell.com)

**Novell®**



Disclaimer      Novell Inc. makes no representations or warranties with respect to the contents or use of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

Trademarks      Novell is a registered trademark of Novell, Inc. in the United States and other countries. All third-party trademarks are property of their respective owner.

Copyright 2007 Novell Inc.

Novell, Inc.  
404 Wyman  
Suite 500  
Waltham  
Massachusetts 02451  
USA

Novell Danmark  
Slotsmarken 12  
2970 Hørsholm

Prepared By      Tommy Petersen  
Senior Technical Specialist  
Certified Information Systems Security Professional (CISSP®)

Novell Nordic Identity and Security Management Team



Novell®



# Content

<b>Preamble.....</b>	<b>1</b>
<b>Comments.....</b>	<b>2</b>
11.4 and potential Liberty value-add/synergies.....	2
12. Product Compliance.....	3
13.6 Requirements for Identity Provider Discovery Profile.....	4
13.7 Name Identifier Management Profile.....	4
13.9 User Attributes to incl. in Authentication Assertion.....	4



**Novell®**



# Preamble

The scope of this document is to provide answers/comments to the hearing opened by IT- og Telestyrelsen on the Danish SAML 2.0 Profile, as defined in the document *SAML Profile for Federation in Danish Public Sector V2.0 (DK-SAML 2.0)*, and its appendix document *Assertion Examples, Version 1.1*.

All information, descriptions or examples herein that relates to a product (COTS) is based on Novells solution for Web Access Management (WAM) and Federation, [Novell Access Manager 3](#).

## 11.4 and potential Liberty value-add/synergies

The latter becomes important as the evolution of DK SAML will begin to encompass the option to allow more granular – user governed – authorizations (DK: fuldmagt), in such a way that individual citizens can grant access to specific private information and change rights to specific groups or individuals within the governmental sector such as Healthcare, Social Services and so on and so forth (see section 11.4 in the hearing document).

The evolution of this functionality is driven by the [Identity Governance Framework](#) initiative driven by Liberty. The hearing document states that it will be considered as it matures into standardization, but the base platform is already well established and we recommend that current COTS implementations of this functionality (– as in Novell Access Manager 3) are deployed to test and evaluate possible **near term** and **long term** implementations.

## 12. Product Compliance

Novell Access Manager 3 is a third generation Web Access Management solutions (COTS) and a second generation platform for federation based on:

- SAML 1.1
- SAML 2.0
- Liberty 1.2 ID-FF (Identity Federation Framework)
- Liberty 1.2 WSF (Web Services Framework)

It supports all operational modes for the Danish SAML 2.0 federation profile as follows:

- Identity Provider (DK-IdP)
- Service Provider (DK-SP)
- Attribute Service (DK-Attr-Svc)

- and its roots in the OASIS SAML 2.0 operational modes.

Novell Access Manager 3 compliance with the SAML 2.0 operational modes is documented in the [Liberty Interoperable](#) testing program. Novell has been deeply involved in the evolution of the SAML 2.0 standard through its involvement with the Liberty Alliance and through being represented on the Liberty Alliance Management Board.

DK-SAML contains specific Danish SAML 2.0 profiles in addition to the adopted subsets of OASIS profiles. These are:

- Authentication Assertion Profile
- OCES Attribute Profile
- Persistent Pseudonym Attribute Profile

- and can be fulfilled through simple configuration of out-of-the-box product functionality. Novell Access Manager 3 further supports:

- Ability to exchange metadata
- Support for persistent pseudonyms
- Ability to opt out of SSO
- Dynamic account linking

- required by the Danish SAML 2.0 profile.

In addition to this Novell Access Manager 3 also supports **Federated Provisioning**, which allows for the automatic policy controlled provisioning of user accounts that do not already exist at the Identity Provider based on SAML. This specific functionality can provide a value add service to the individual user (citizen, employee etc.) and to the governmental sector as a whole, where user identities for the purpose of single sign-on access to external (non-government or foreign etc.) organizations can be provided in a standardized, controlled and secure manner.

## 13.6 Requirements for Identity Provider Discovery Profile

Novell Access Manager 3 also supports the Identity Provider Discovery Profile.

## 13.7 Name Identifier Management Profile

The potential value of Name Management lies in how the system manages the sharing of common identifiers for a principal between identity and service providers. When an identity provider has exchanged a persistent identifier for the principal with a service provider, the providers share the common identifier for a length of time. When either the identity or service provider changes the format or value to identify the principal, the system can ensure that the new format or value is properly transmitted, which potentially can become important in a distributed infrastructure with multiple authoritative sources.

The Name Identifier Management Profile is part of SAML 2.0 and is supported by Novell Access Manager 3 as is both SOAP and HTTP Post/Artifact bindings.

## 13.9 User Attributes to incl. in Authentication Assertion

Taking not only necessary core user attributes to complete authentication assertions into consideration, the potential of Federated Provisioning should be considered and the basic attribute requirements for user object creation in the most predominant directories/name systems in the governmental sector.

Since Federated Provisioning is considered to gain importance, either the COTS products will have to support (policy controlled) string constructing in order to build required attribute information from existing core attributes **or** the core user attribute list should be extended. The aforementioned functionality could also potentially remove the requirement to have the uid attribute as a core requirement, since this information could be constructed based on f.ex. first letter of common name (cn) concatenated with surname (sn).