



DNSSec

Ulrich Wisser

Developer

.SE Internet Infrastructure Foundation

.se

User Interface

The screenshot displays the .se DomainManager web interface. The top navigation bar includes the .se logo, the text "DomainManager", and links for "Customer service", "Help pages", and "Logout". On the left, a sidebar menu lists various account management options. The main content area is titled "Domain | wisser.se" and features a tabbed interface with "Overview", "Contacts", "Nameservers", "DNSSEC", and "History". The "Overview" tab is active, showing general domain information. Below the tabs, a text block explains that general information is shown and provides instructions for accessing more detailed data. A table titled "Information" lists key domain details. At the bottom of the main content area, there are links to "Cancel the domain", "Cancel DNSSEC service", "See help section", and "Print".

.se DomainManager Customer service Help pages Logout

Account
Logged in: Www Publisher
Customer number: 79620921

Start page
Domains
Contact information
Payment notification
Account settings
Messages
Search tools
Bulk change

Domain | wisser.se

Overview Contacts Nameservers DNSSEC History

General information about the selected domain name is shown below. If you want to view more detailed information or change something, such as adding or removing a contact or changing the name server, click on one of the tabs above.

Information

Domain name	wisser.se
Holder	WORLD WIDE WEB PUBLISHER ULRICH WISS (wwwpub0702-00001)
Status	Active
Date created	2003-04-24
Due date	2009-04-24
Selected registrar	Loopia AB

Select a registrar

Cancel the domain Cancel DNSSEC service

See help section Print

.se

User Interface

.se | DomainManager

Customer service | Help pages | Logout

Account

Logged in: Www Publisher
Customer number: 79620921

Start page

Domains

Contact information

Payment notification

Account settings

Messages

Search tools

Bulk change

Domain | **wisser.se**

Overview | Contacts | Nameservers | **DNSSEC** | History

The listing below contains the DNSSEC keys linked to your domain. If you want to publish keys in the .se zone, or unpublish previously published ones, please check or uncheck those keys and click "Update key list".

Note that this can only be made if you are Holder, Technical contact or Administrative contact for the domain name.

Status	Key tag	Algorithm	Fingerprint (SHA-1)	Key type
☒ Published	33622	RSA/SHA-1	57443EC5F08EB35752A	KSK
☐ Non publishable	38967	RSA/SHA-1	A65B7B7BCD7F4D51A	ZSK
☐ Non publishable	63357	RSA/SHA-1	78A00F3AB7847FB627F	ZSK

Update key list

Reset

See help section

Print

.se

User Interface

Domain | **wisser.se**

Overview

Contacts

Nameservers

DNSSEC

History

The listing below contains the DNSSEC keys linked to your domain. If you want to publish keys in the .se zone, or unpublish previously published ones, please check or uncheck those keys and click "Update key list".

Note that this can only be made if you are Holder, Technical contact or Administrative contact for the domain name.

Status	Key tag	Algorithm	Fingerprint (SHA-1)	Key type
☒ Published	33622	RSA/SHA-1	57443EC5F08EB35752A	KSK
☐ Non publishable	38967	RSA/SHA-1	A65B7B7BCD7F4D51A	ZSK

- ★ Zone key flag is set.
- ★ The secure entry point (SEP) flag is not set.
- ★ The protocol is version 3.
- ★ The algorithm is correct.
- ★ The zone is signed.
- ★ The algorithm is considered secure.
- ★ Known algorithm.
- ★ Bits 0-6 and 8-14 is zero.

☐ Non publishable	63357	RSA/SHA-1	78A00F3AB7847FB627F	ZSK
--	-------	-----------	---------------------	-----

Update key list

Reset

.se

User Interface

Domain | **wisser.se**

Overview

Contacts

Nameservers

DNSSEC

History

The listing below contains the DNSSEC keys linked to your domain. If you want to publish keys in the .se zone, or unpublish previously published ones, please check or uncheck those keys and click "Update key list".

Note that this can only be made if you are Holder, Technical contact or Administrative contact for the domain name.

Status	Key tag	Algorithm	Fingerprint (SHA-1)	Key type
☒ Published	33622	RSA/SHA-1	57443EC5F08EB35752A	KSK 
★ Zone key flag is set. ★ The secure entry point (SEP) flag is not set. ★ The protocol is version 3. ★ The algorithm is correct. ★ The zone is signed. ★ The algorithm is considered secure. ★ Known algorithm. ★ Bits 0-6 and 8-14 is zero.				
Non publishable	38967	RSA/SHA-1	A65B7B7BCD7F4D51A	ZSK 
Non publishable	63357	RSA/SHA-1	78A00F3AB7847FB627F	ZSK 

Update key list

Reset

.se

User Interface

.se DomainManager

Customer service Help pages Logout

Account
Logged in: Www Publisher
Customer number: 79620921

Start page

Domains

Contact information

Payment notification

Account settings

Messages

Search tools

Bulk change

Domain wisser.se

Overview Contacts Nameservers DNSSEC History

The history for the selected domain name is listed below.

Type	Event	Object	Date
DNSSEC	Added	keytag:33622 Algorithm:5	2008-05-15 10:22:24
DNSSEC	Removed	all DNSSEC keys	2008-05-15 10:22:24
DNSSEC	Removed	all DNSSEC keys	2008-05-15 10:22:23
DNSSEC	Reactivated	DNSSEC service	2008-05-15 10:22:23
Nameserver	Added	dnssec2.loopia.se	2008-05-15 09:44:17
Nameserver	Added	dnssec1.loopia.se	2008-05-15 09:44:17
Nameserver	Removed	ns3.loopia.se	2008-05-15 09:44:17
Nameserver	Removed	ns4.loopia.se	2008-05-15 09:44:17
Domain		wisser.se	2008-04-10 06:51:28
Domain		wisser.se	2007-04-11 06:37:03

1 2 30 30 30

Post 1 - 10 (of totally 12 entries).

[See help section](#) [Print](#)

.se



Trust is good, control is better.

- Key exchange needs trust and control
- Reuse existing trust channels
- Use DNS for key control
- Provide extended security

.se



Key Control

- The Zone Key flag must be set (Bit 7).
- The Secure Entry Point flag must be set (Bit 15).
- The other bits of the flag field should be zero.
- Protocol must be "3".
- The algorithm must not be marked as reserved (0, 255).
- The key must sign all keys in the zone.
- Algorithm RSA/MD5 (1) shouldn't be used.
- Algorithm should be known (1-5).
- The algorithm should be RSA/SHA-1 (5).

.se



Extended security

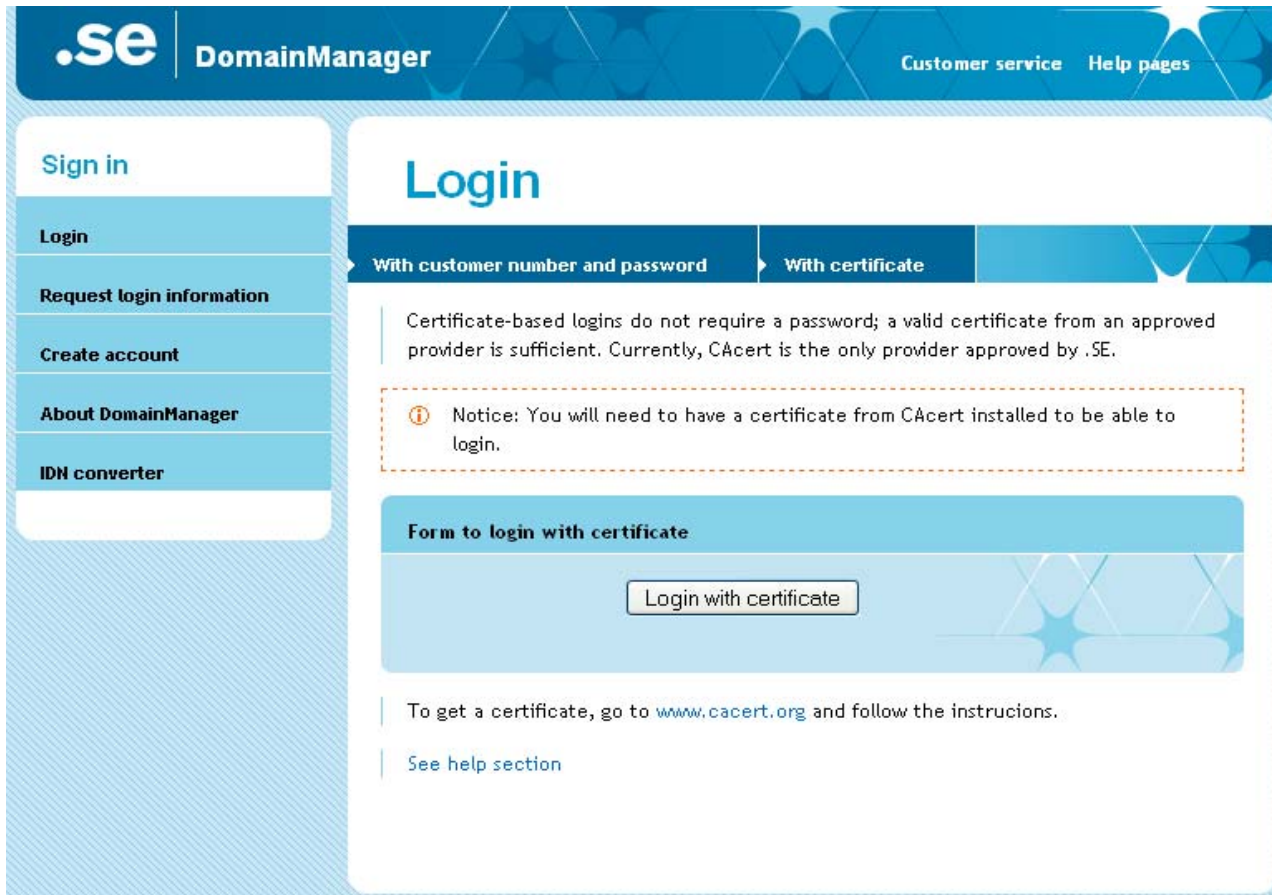
- Passwords are weak
- Password recovery through email
- Provide alternative (more secure) login process
- Use digital certificates for identification

Problems

- Login is part of the application
- Building in several login processes makes login complex.
- Complex software => more errors

.se

Certificate Login



The screenshot shows the .se DomainManager login interface. On the left is a sidebar with links: Sign in, Login, Request login information, Create account, About DomainManager, and IDN converter. The main content area is titled 'Login' and has two tabs: 'With customer number and password' (selected) and 'With certificate'. Below the tabs, a text block explains that certificate-based logins do not require a password and that CACert is the only approved provider. A dashed orange box contains a notice: 'Notice: You will need to have a certificate from CACert installed to be able to login.' Below this is a section titled 'Form to login with certificate' containing a 'Login with certificate' button. At the bottom, there are links to get a certificate from www.cacert.org and to see the help section.

.se DomainManager Customer service Help pages

Sign in

- Login
- Request login information
- Create account
- About DomainManager
- IDN converter

Login

With customer number and password **With certificate**

Certificate-based logins do not require a password; a valid certificate from an approved provider is sufficient. Currently, CACert is the only provider approved by .SE.

Notice: You will need to have a certificate from CACert installed to be able to login.

Form to login with certificate

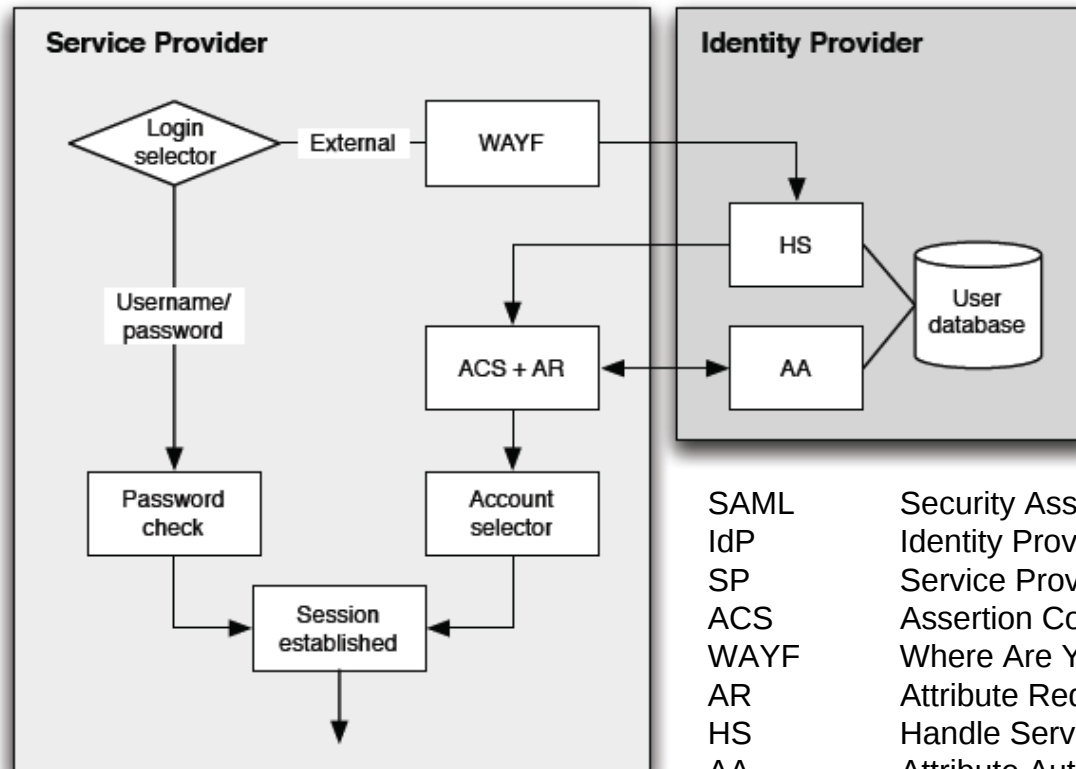
Login with certificate

To get a certificate, go to www.cacert.org and follow the instructions.

[See help section](#)

.se

Identity provider



SAML
IdP
SP
ACS
WAYF
AR
HS
AA
SSO

Security Assertion Markup Language
Identity Provider
Service Provider
Assertion Consumer Services
Where Are You From
Attribute Requestor
Handle Service
Attribute Authority
Single-Sign On

.se



Experiences

- Only supports CACert
- IdP Software is really, really complex
- XMLsig handling is not fully supported
- Certificate handling between IdP and SP
- Hard to monitor IdP, certificates
- Customer support "doesn't get it"
- If it works, it's perfect! 😊

.se



Thank you!

Ulrich Wisser

Developer

.SE Internet Infrastructure Foundation

.se