DNSSec

Ulrich Wisser

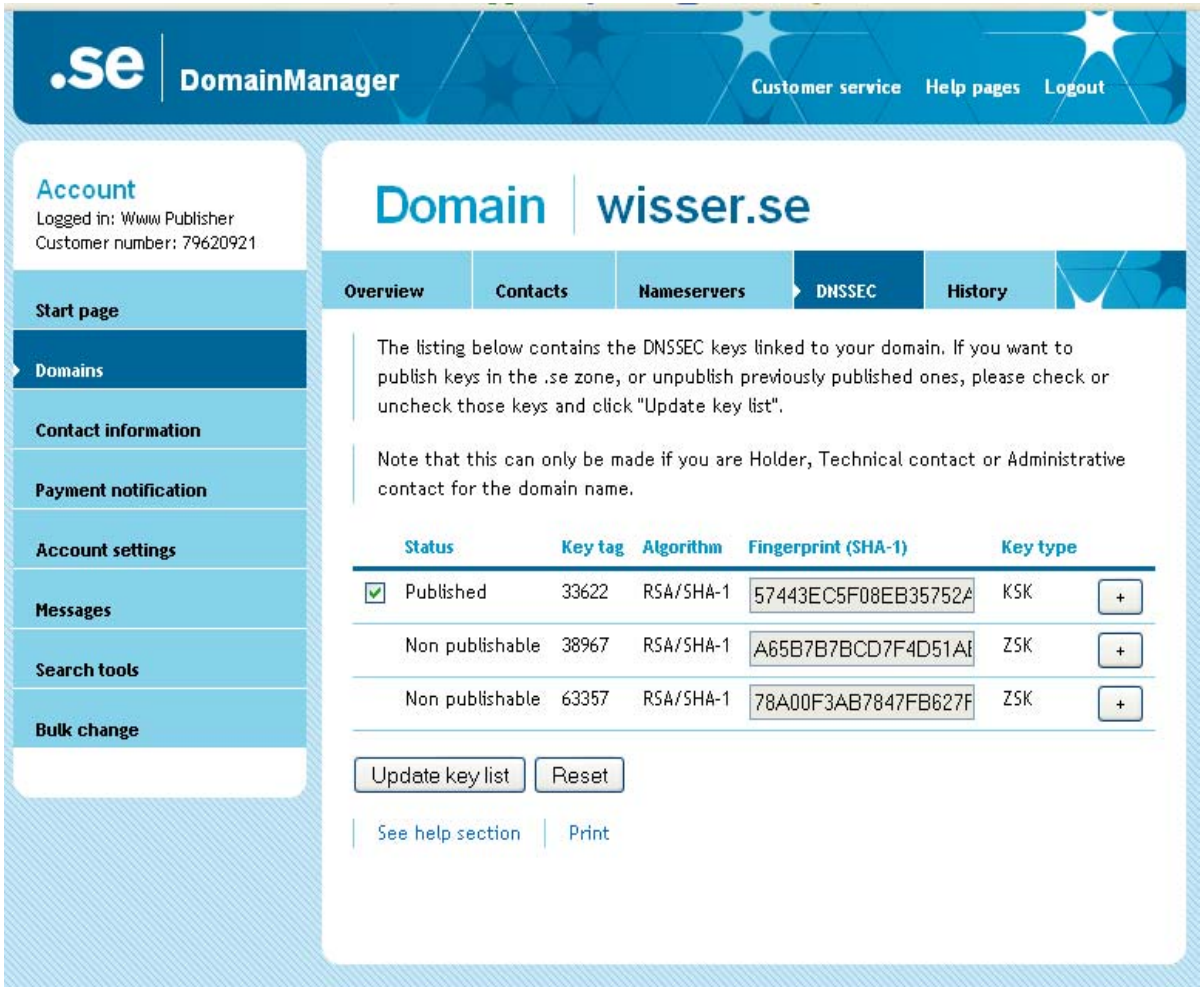
Developer

.SE Internet Infrastructure Foundation

User Interface

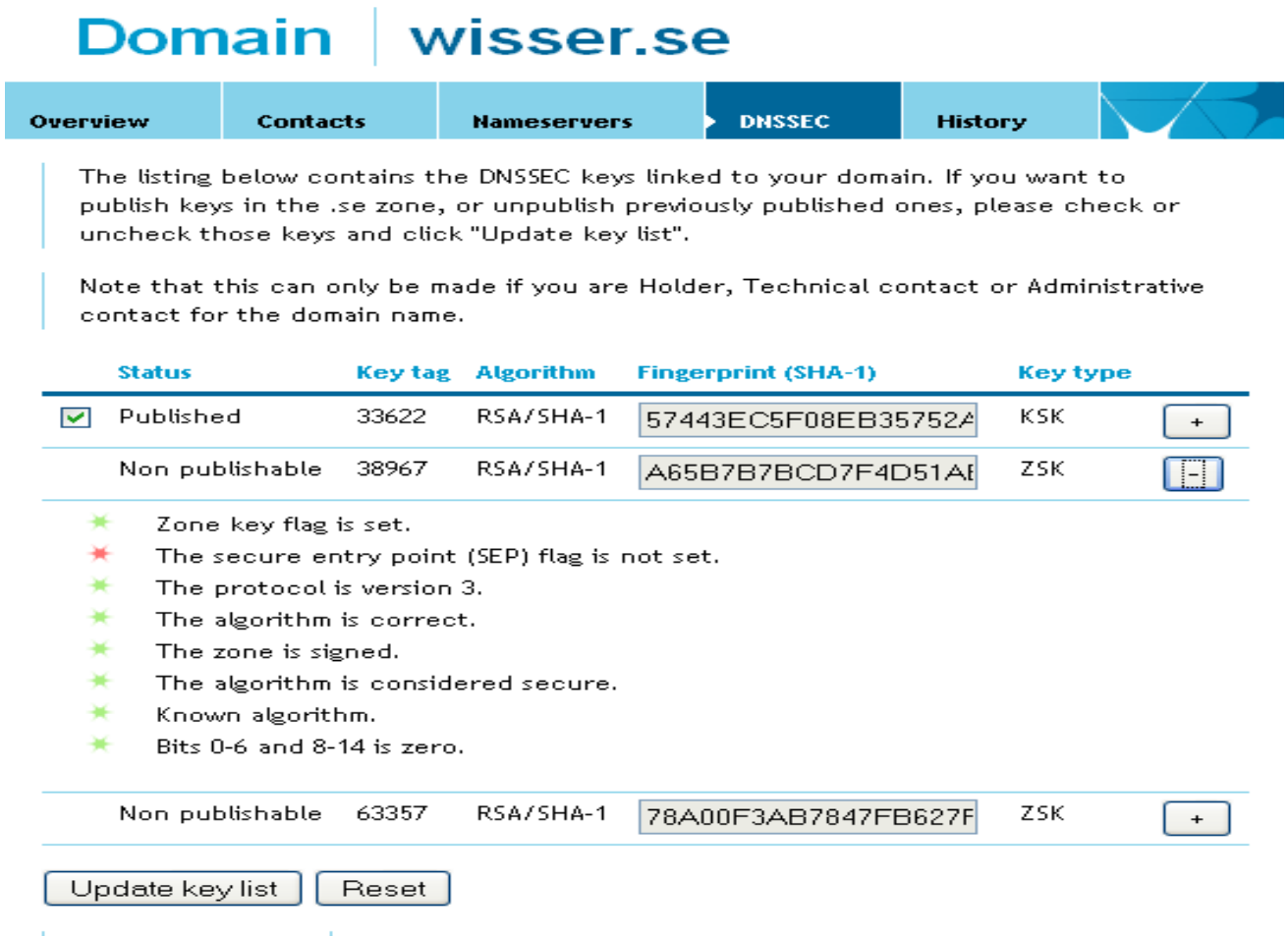
.se

User Interface



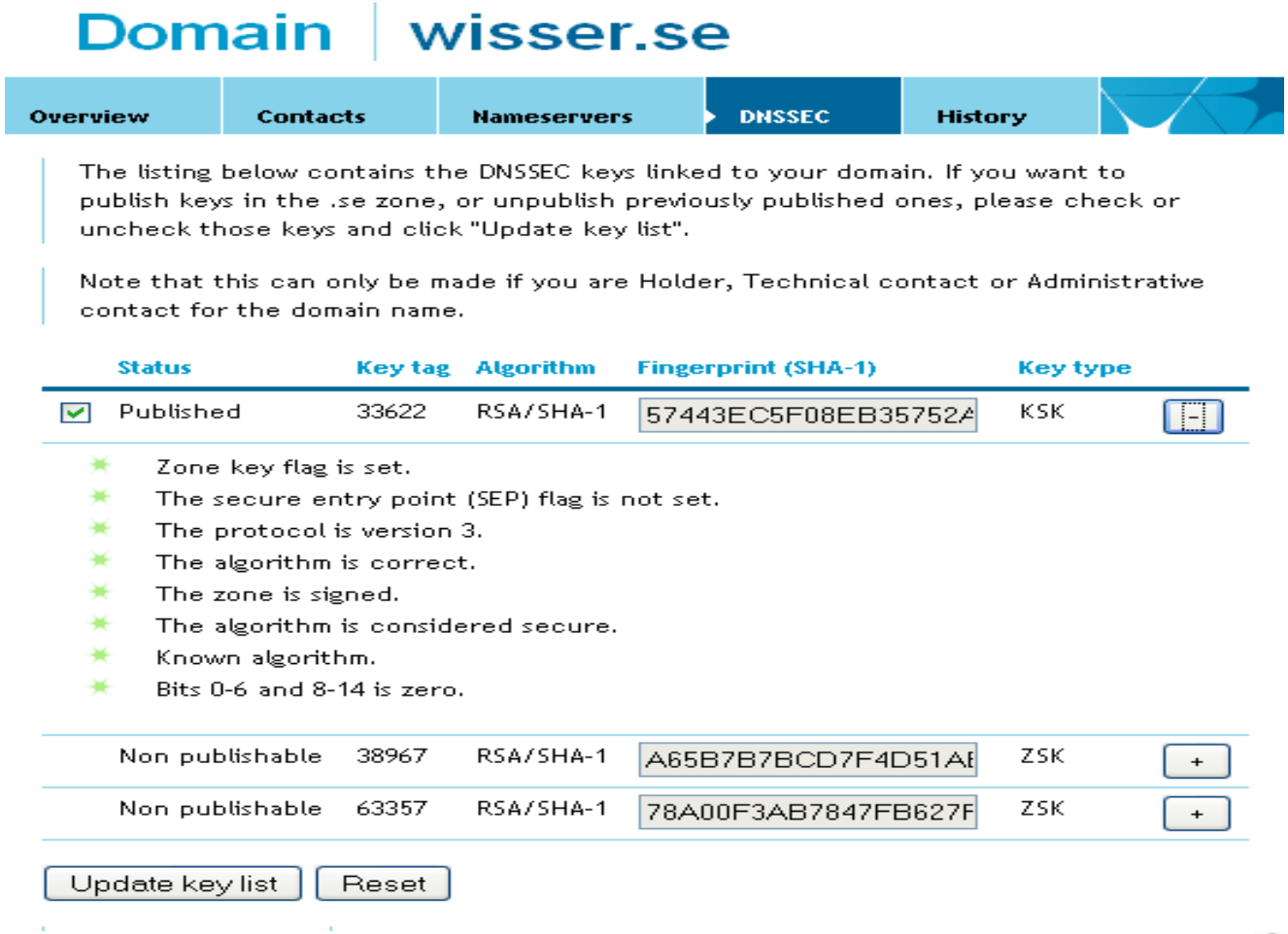
.se

User Interface



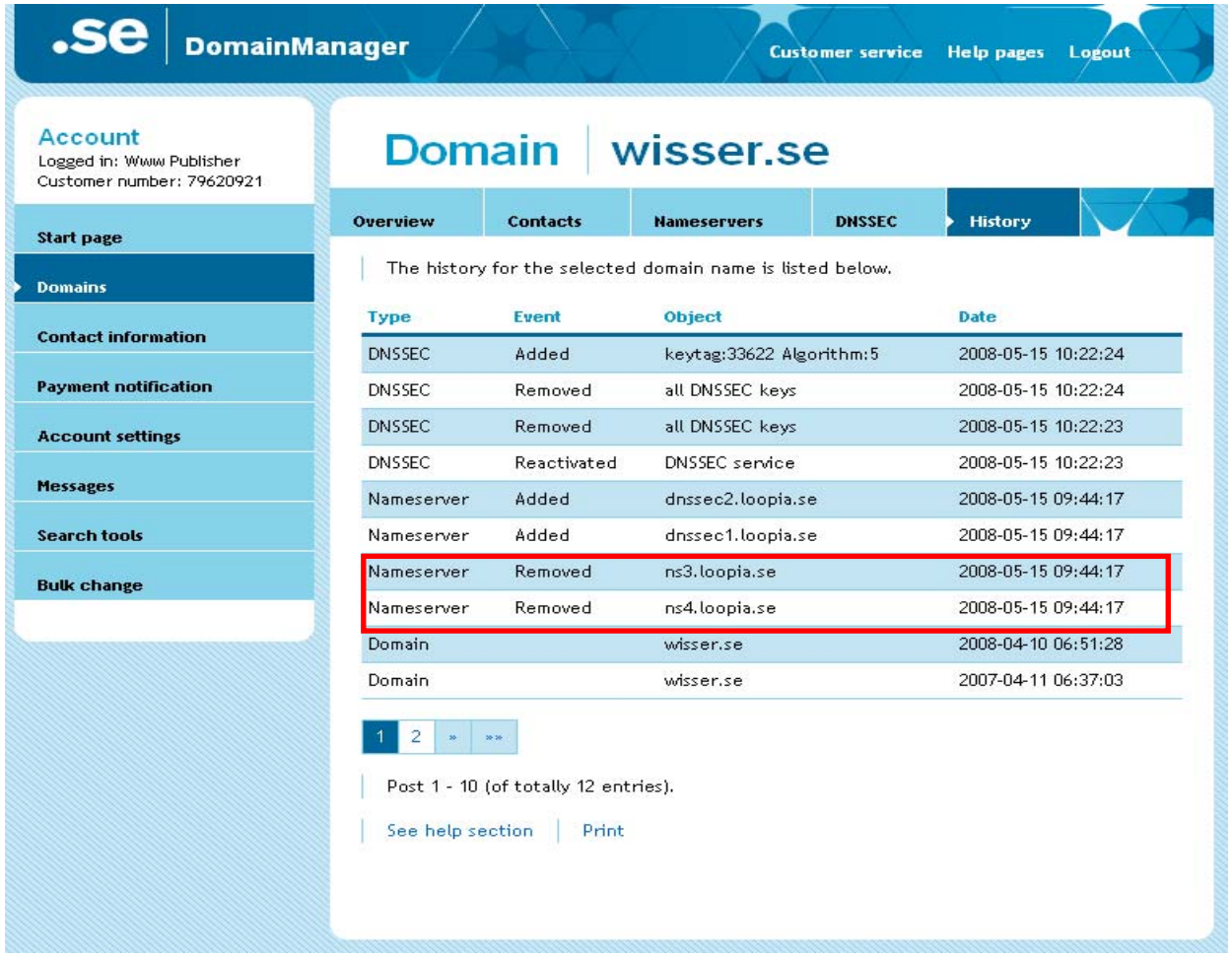
.se

User Interface



.se

User Interface



.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 be 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

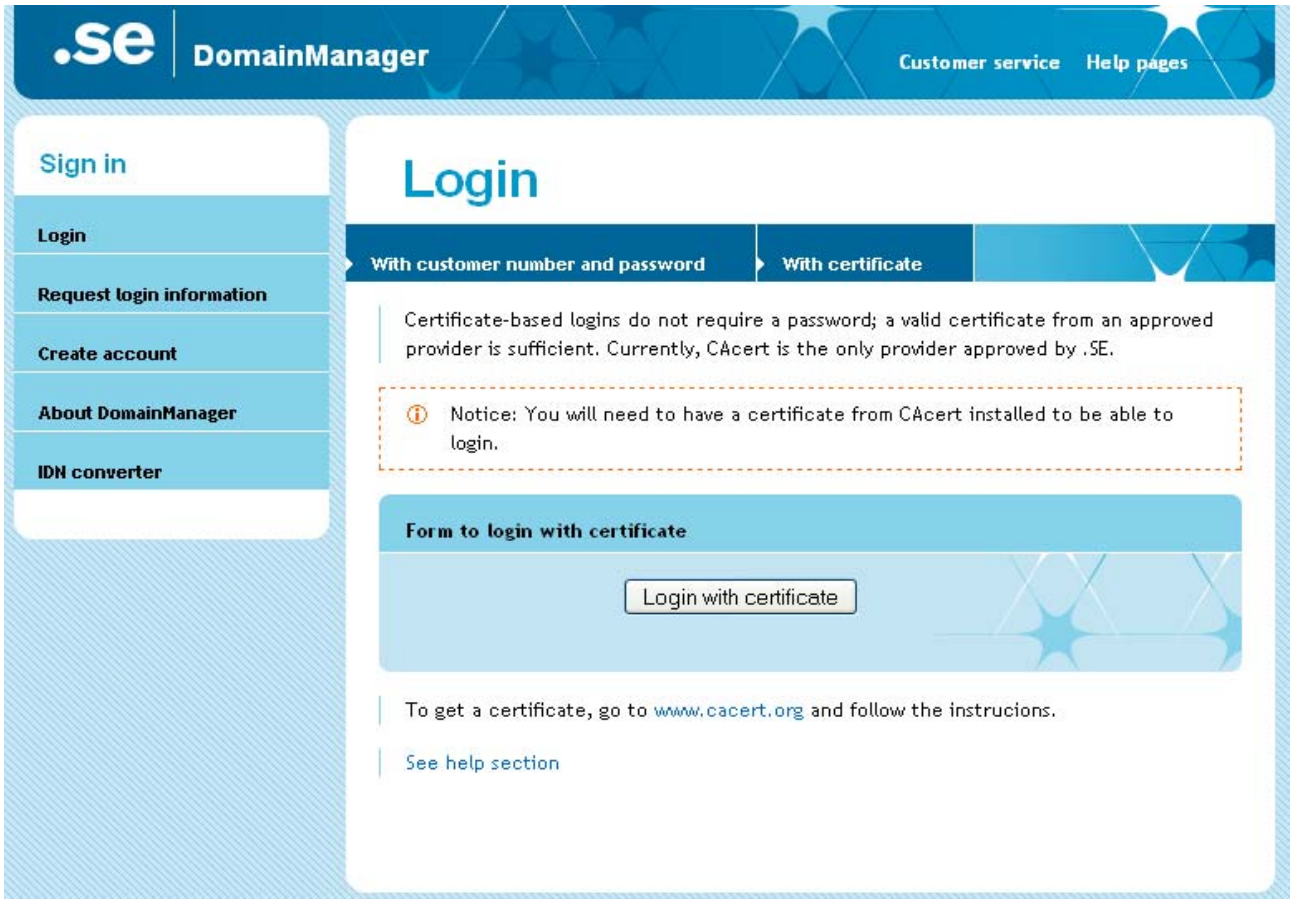
- Passwords are weak
- Password recovery through email
- Provide alternative (more secure) login process
- Use digital certificates for identification

Problems

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

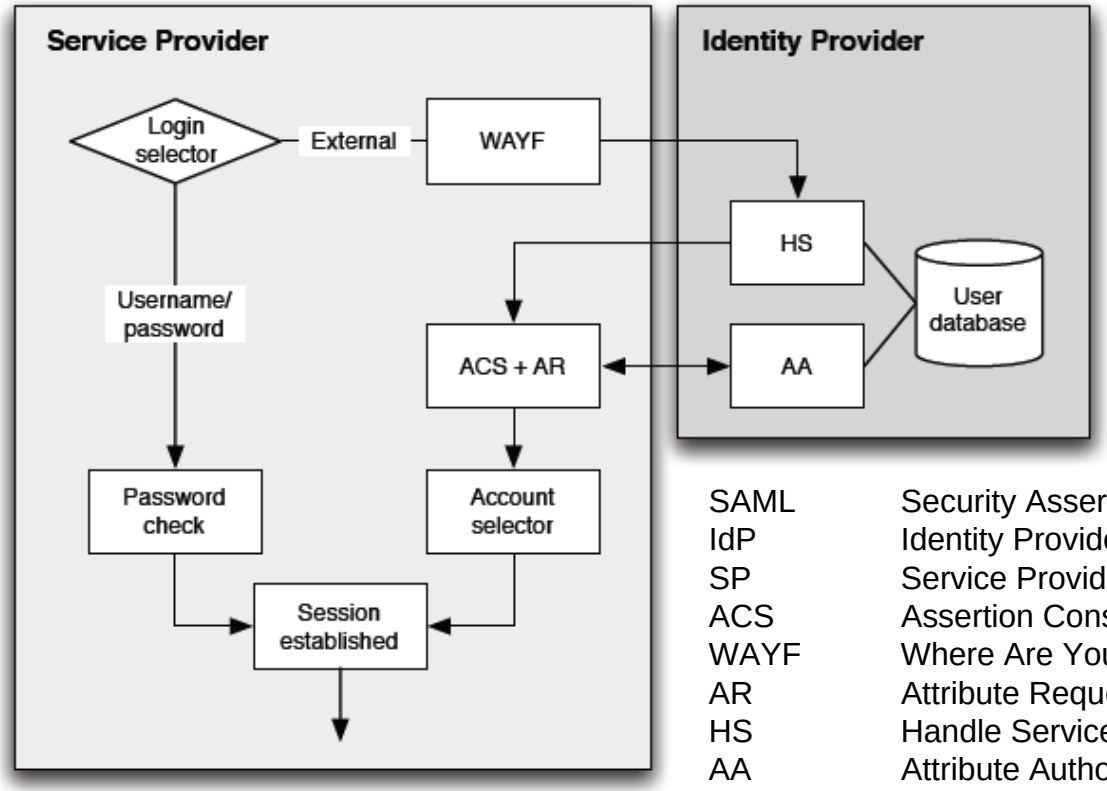
.se

Certificate Login



.se

Identity provider



SAML	Security Assertion Markup Language
IdP	Identity Provider
SP	Service Provider
ACS	Assertion Consumer Services
WAYF	Where Are You From
AR	Attribute Requestor
HS	Handle Service
AA	Attribute Authority
SSO	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