Cross-over workshop
Registrar Identification and Authentication

Anne-Marie Eklund Löwinder, CISO, .SE
amel@iis.se
@amelsec
Agenda for the afternoon

13.00  Introduction (Anne-Marie Eklund Löwinder, .SE)

13.20  Roundtable - Members expectations and experiences

13.50  Examining current scenarios: what problem are we trying to solve? (Kristof Tuyteleers, DNS Belgium)

14.10  IANA Experience (Kim Davies, IANA)

14.30  Coffee break

14.50  Future scenario: Secure registrar identification and authentication in Europe (Fredrik Ljunggren, Kirei and Ulrich Wisser, .SE)

15.50  Drafting registrar survey

16.30  Next steps - To do's

17.00  Closing
Security incidents

- 9.10.2012 .ie  google.ie hijacked
- 24.11.2012 .pk
- 28.11.2012 .ro
- 5.12.2013 .rs  multiple domains hijacked
- 5.7.2013 .be  Web defacement
- 5.7.2013 .nl  Malware distribution via Website
- 27.7.2013 .be  Website
- 5.8.2013 .nl  Registrar Credentials compromised
- 25.8.2013 .ps  Google Maps
- 8.10.2013  avira.com Network Solutions - fake password-reset
- 19.10.2013  entire .qa DNS hijacked
Why this will continue

- Domain names are the key to resources on the internet
- These resources are mostly better protected than the $10 domain name
- Domain name business is a mass market
- One registrar account gives access to 1000s of domains
- Access control relies on userid & password
How to avoid DNS hijacking

- Registry/Registrar lock
- Select your registrar or domain reseller
- Strong authentication
- Control access to your DNS
- Monitor DNS records
- Use DNSSEC
Workshop

- We need to identify the registrar in a more secure way. How?
- What is the lowest acceptable level of authentication?
- What are the common requirements and available solutions for identification and authentication of registrars?
- What is the next step?