Cloud security
at OASIS International Cloud Symposium,
London, October 10, 2011

Marnix Dekker, ENISA
Security ❤ Standards
SAML Transaction Steps

1. User tries to reach hosted Google application
2. Google generates SAML request
3. Google redirects browser to SSO URL
4. Partner parses SAML request, authenticates user
5. Partner generates SAML response
6. Partner returns encoded SAML response to browser
7. ACS URL
   - ACS verifies SAML response
8. User is logged in to Google application
Cloud standardizes IT
Security ♥ Cloud
Cloud computing risk assessment

- Information security risks and opportunities
Elastic
Green
Off-premise (sometimes abroad)
Resource concentration
Leverage
Specialists
Trust
ENISA’s cloud work

- 2009 Cloud computing risk assessment
- 2009 Cloud security control framework
- 2011 Security and resilience for gov clouds
- 2011 Security parameters in gov cloud SLAs
- 2011 EU Cloud strategy
- 2012 Critical clouds
Cloud security; if you can’t measure it, you can’t manage it.

(Securely juggling SLAs for IT officers)
The proof is in the eating...
Governance and assurance standards
Secure your website with award-winning SSL products!

SSL CERTIFICATES from only $29/year

Host Color partners Comodo, a leader in Internet security to provide high quality SSL certificates!
Workshop on security in cloud SLAs

- Chaired by ENISA, OASIS, CSA
- October 13th, London, 10:00 to 13:00
- Hands-on, the result will be a co-authored draft of best practices
- Lunch provided
Contact
Marnix Dekker (marnix.dekker@enisa.europa.eu)
Giles Hogben (giles.hogben@enisa.europa.eu)

About securely moving to smartphones and cloud computing
http://www.enisa.europa.eu/act/application-security

Upcoming events
• Joint ENISA, OASIS, CSA Workshop on security in cloud SLAs (October 13th, London)
• Virtual ENISA working group: Best practices for Cloud SLAs
• SecureCloud 2012 (ENISA, CSA, Fraunhofer)