Teleworking and access to ECHA IT systems

Biocides CA meeting
16 May 2013

Hugues KENIGSWALD

Background

- The same security model is used to access both REACH/CLP and Biocides data
  - Unified Security Declaration of Commitment
  - Standard Security Requirements (SSR)
- Teleworking proposal discussed with the Security Officers' Network (SON) on 15 May 2013
- If agreement reached by SON, it is foreseen that ECHA Management Board amends the SSR to allow teleworking in its June 2013 meeting

Proposal

Implementation

- two examples of practical implementation of the teleworking rules:
  - Teleworking solution already in place (Option 1)
  - Direct access to ECHA (Option 2)

Teleworking rules

- Policies on teleworking responsibilities and user behaviour including a signed agreement
- Processes on security awareness, software updates and security reporting and response
- Technical controls on identifying equipment, encrypting data, firewall, anti-virus and wireless connections as well as authorised software and users

Further details

Risks and mitigating measures

Client devices

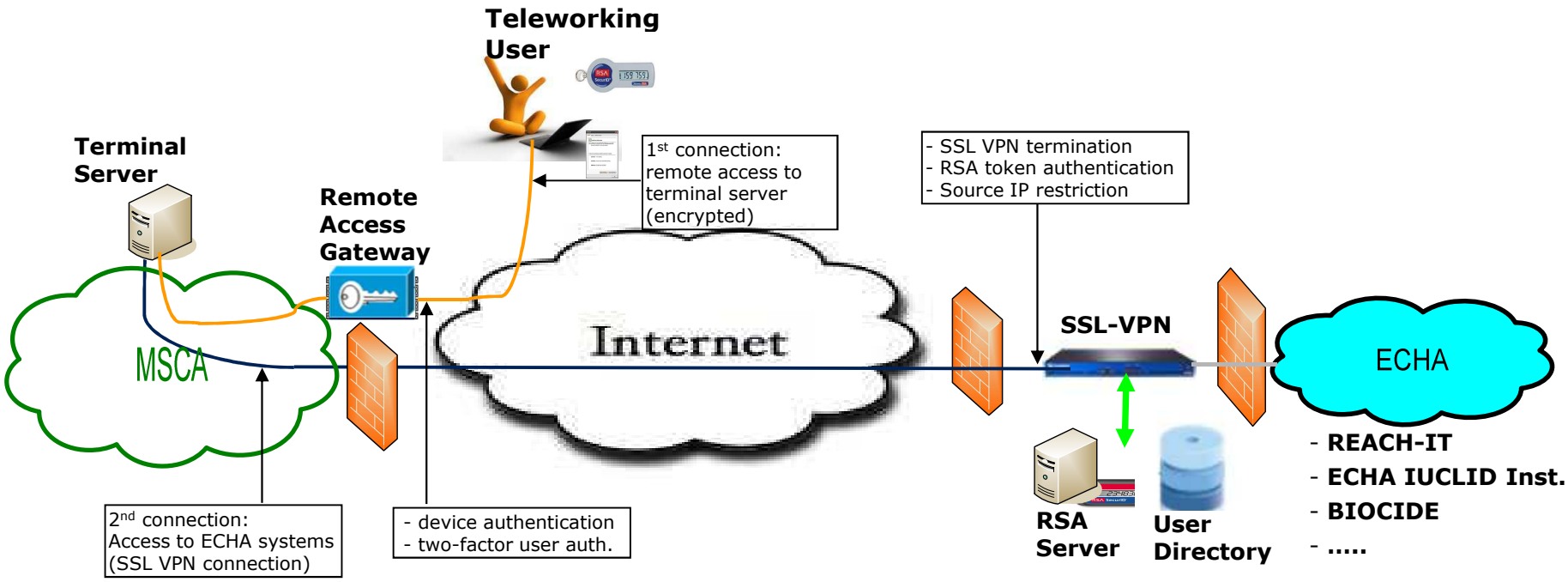
RISK	*RULES to mitigate the risk*
A telework device which contains confidential data is lost and stolen	Hard drives and portable storage devices must be encrypted using password with complexity requirements Incident reporting and response process must be in place A clean screen policy: screen must be locked
Confidential information stored or processed on (a shared) client device is accessible for other users	Equipment must be reliably authenticated Equipment may be used only by authorised users based on business need-to-know principle A teleworking policy must be in place
A device is infected by a malware which steals confidential data stored or processed on the device	The equipment must have up-to-date anti-virus software and virus definitions Client firewall enabled , control which applications are allowed to initiate outbound network connections Software installed on the equipment has reasonable business justification
Unauthorised access to the remote service by intruding to a device with an active connection (e.g. VPN tunnel)	Client firewall enabled with reasonably restrictive (especially inbound) rules Software installed on the equipment has reasonable business justification

Teleworking and remote access

RISK	*RULES to mitigate the risk*
Unauthorised access to remote service by hijacking a valid connection	No unprotected wireless networks may be used
Unauthorized access to remote service, which is available from anywhere, is exploited	Logging and monitoring process must be in place to detect unusual activity A Non Disclosure Agreement (NDA) must be signed by each authorised user (passwords or other authentication credentials are not revealed, or shared with others)
Confidential data on screen is overseen	A clean screen policy must be in place, that is equipment screen must be locked when not in use A teleworking policy must be in place
Unauthorized access to confidential data in paper format	A clean desk policy must in place (store information in locked cabinets, print-outs outside the protected premises cannot be left unprotected or unattended) A teleworking policy must be in place

Practical Implementation Options

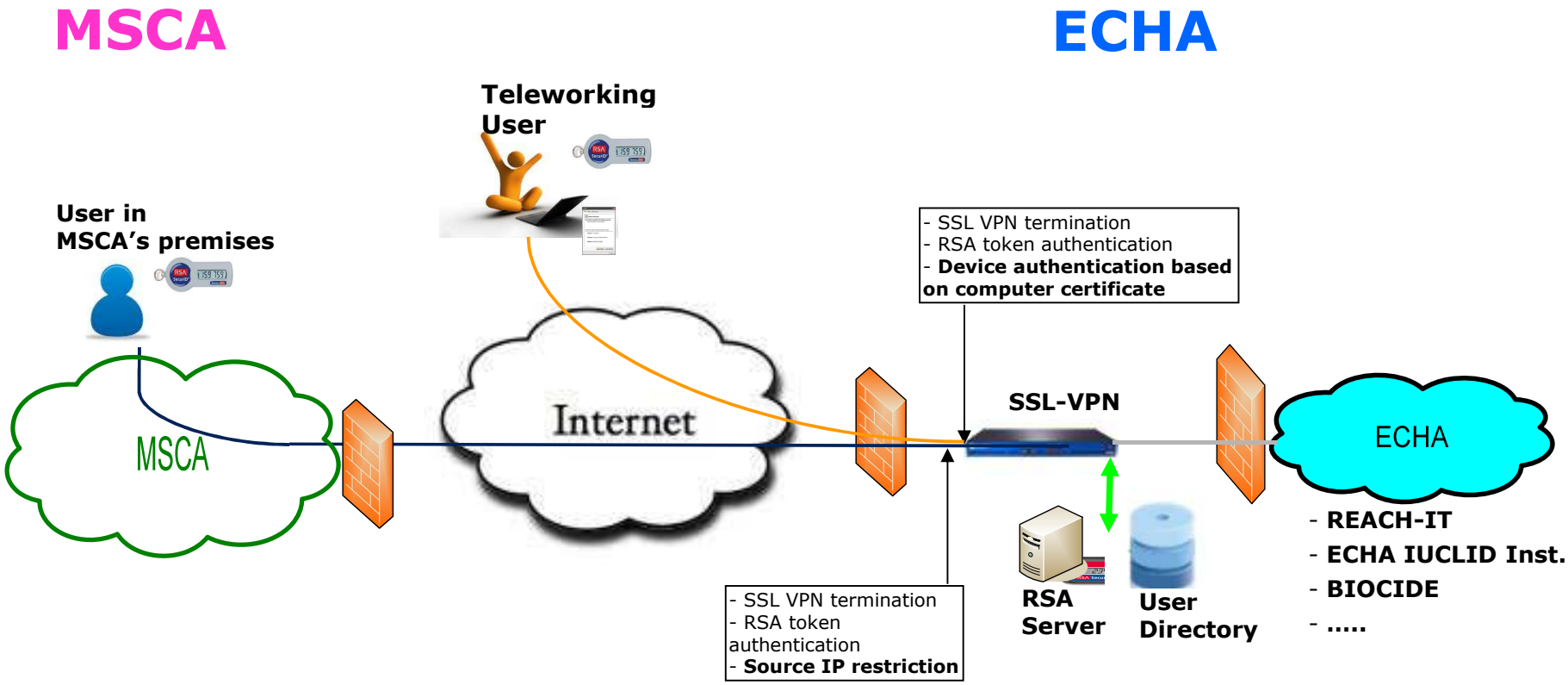
Option 1: Terminal Server at MSCA



Option 1: Terminal Server at MSCA

- Remote access solution for telework is fully implemented and maintained by the MSCA
  - The MSCA is in charge to implement it in line with security rules
- ECHA sees no difference between telework connections via Terminal Server and standard connections from the office premises
- This option is recommended if the MSCA already has a remote access solution (and Terminal Server) in place

Option 2: Direct access to ECHA



Option 2: Direct access to ECHA

- Telework clients establish connection directly to the dedicated interface on ECHA's remote access gateway
  - No source IP restriction
  - Device authentication based on computer certificates
- MSCA has to install and manage computer certificates
  - A client application is needed for the device authentication
  - ECHA's remote access gateway accepts device certificates which are issued by a trusted MSCA Certificate Authority (CA)
- Recommended if MSCA
  - has no remote access solution in place
  - is able to manage computer certificates
- Please note that the device authentication with computer certificates sets limitations for client systems