Italian server-based qualified signature
UNINFO SC FIS

• Within the Italian standardization framework UNINFO is the national standardization body for ICT
• FIS is a Subcommittee within the TC "Information technology - Security techniques" the Italian mirror of ISO SC27
• SC FIS ToR include standardization related activities on eSignature, eSeals, eID and related devices and services:
  – provide contributions to ETSI/ESI, CEN WG15 & WG17 and ISO SC27
  – propose the vote as NSO when required (ETSI, CEN, ISO)
  – produce national standards when needed (i.e. no standards already exist)
• SC FIS participation is open to any interested stakeholder, public and private organizations, among which:
  – AgID (Agenzia per l'Italia Digitale, formerly DigitPA/CNIPA): the Italian TSP Supervision authority
  – OCSI (Organismo di Certificazione della Sicurezza Informatica): the national Common Criteria certification body
CSP Supervision and SSCD Certification

Signature Directive (99/93/EC) - Article 4 - Market Access

• Article 4(3) Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public -> in Italy: AgID - Agenzia per l'Italia Digitale

• Article 4(4) The conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States. [...] A determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph shall be recognised by all Member States. -> in Italy: OCSI - Organismo di Certificazione della Sicurezza Informatica

• Article 4(5) The Commission may [...] establish and publish reference numbers of generally recognised standards for electronic-signature products [...]. Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards. -> to date, only CWA 14169 is generally recognized in EU for SSCDs
Server based signing - Typical scenarios

1. "automatic signature"
   unattended signature of documents (e.g. certifications, electronic invoicing, etc.).
   Scenario similar to typical CSP operation
   -> few signers often operating near the HSM

2. "remote signature"
   Signature of few documents by many users
   (e.g. enterprise workflows, home banking)
   -> many signers operating remotely
SSCD assessment procedure

• CWA 14169 Protection Profile: security requirements for an SSCD implemented as Smart Card

• CWA 14167 Protection Profile: security requirements for HSMs used by CSP for their operations (such as signing of Certificates, Time-Stamp tokens, etc)

• An assessment procedure has been defined by OCSI to establish if a signature creation device conforms to Annex III of Directive 99/93/EC

• When the device passes the assessment procedure a Conformity Attestation and an Assessment Report are released
Device assessment as SSCD

Is a standard PP applicable, such as CWA 14169?

- **YES**
  - Standard CC certification

- **NO**
  - Already CC Certified?
    - **YES**
      - Assessment procedure Type 1
    - **NO**
      - Assessment procedure Type 2
Assessment procedure Type 1

- This procedure applies to devices already Common Criteria certified, but not as SSCD
- An example is a CWA 14167 certified HSM (even if CC EAL4+ certified this do NOT imply it is an SSCD)
- OCSI evaluates if and under which (additional) conditions the device can be used as an SSCD
- The Conformity Attestation, together with the device Common Criteria certification and the OCSI Assessment Report, specify the operating conditions to comply with the Annex III of the Directive
- AgID as supervisory body is responsible for:
  - assessing specific implementation compliance with its CC certification report and, eventually, the additional SSCD constraints required by OCSI
  - implementation compliance periodical surveillance
Assessment procedure Type 2

- This procedure applies to device ready for a Common Criteria certification process presenting to OCSI its Security Target
- OCSI preliminary evaluates the device Security Target and approve it as **SSCD compliant** if, together with other requirements specified in OCSI conformity assessment procedure, Directive Annex III security requirements are met
- If the device achieve **CC EAL4+ certification** according to the approved final version of the ST then it can be used as SSCD in all EU
- Accredited Italian CSPs that intend to provide server side signature services can self declare the conformity of solutions based on devices for which:
  - OCSI assessment procedure on ST was started before Nov 1, 2011
  - on Jan 25, 2013 the assessment was successfully completed and the CC certification process has been started on the approved ST
- AgID as **supervisory body** is responsible for:
  - assessing specific implementation compliance with its CC certification report
  - implementation compliance periodical surveillance
"Pre-verified" signature

• A server based signature that is:
  – compliant with the Signature Directive requirements, i.e. a certified signature device activated under sole control by the signatory
  – available only if the corresponding certificate is valid at signature time (not revoked, suspended or expired) - real time check
• no general need to check the certificate status client side - after evaluation of the risk in each context
• the signature contains a reliable time mark put by the CSP (as trustable as a time-stamp token)
• Pre-verified signature will be introduced in Italy with a new set of legal rules under approval
Pre-verified signature certificates

• The pre-verified signature service (including the signature device) is operated by qualified and accredited CSPs and under surveillance of the supervision body

• The signature device is CC certified and a compromise can be dealt like a CSP compromise (revocation of CA key/change status in the Trust List)

• Use of a specific additional QC Statement seems the most simple solution to allow signature verification applications to recognize pre-verified signatures

• A signature verification application can ignore the QC Statement and apply the general verification process
Thanks!