STORK as a foundation for the eIDAS e-ID architecture

Antonio Lioy

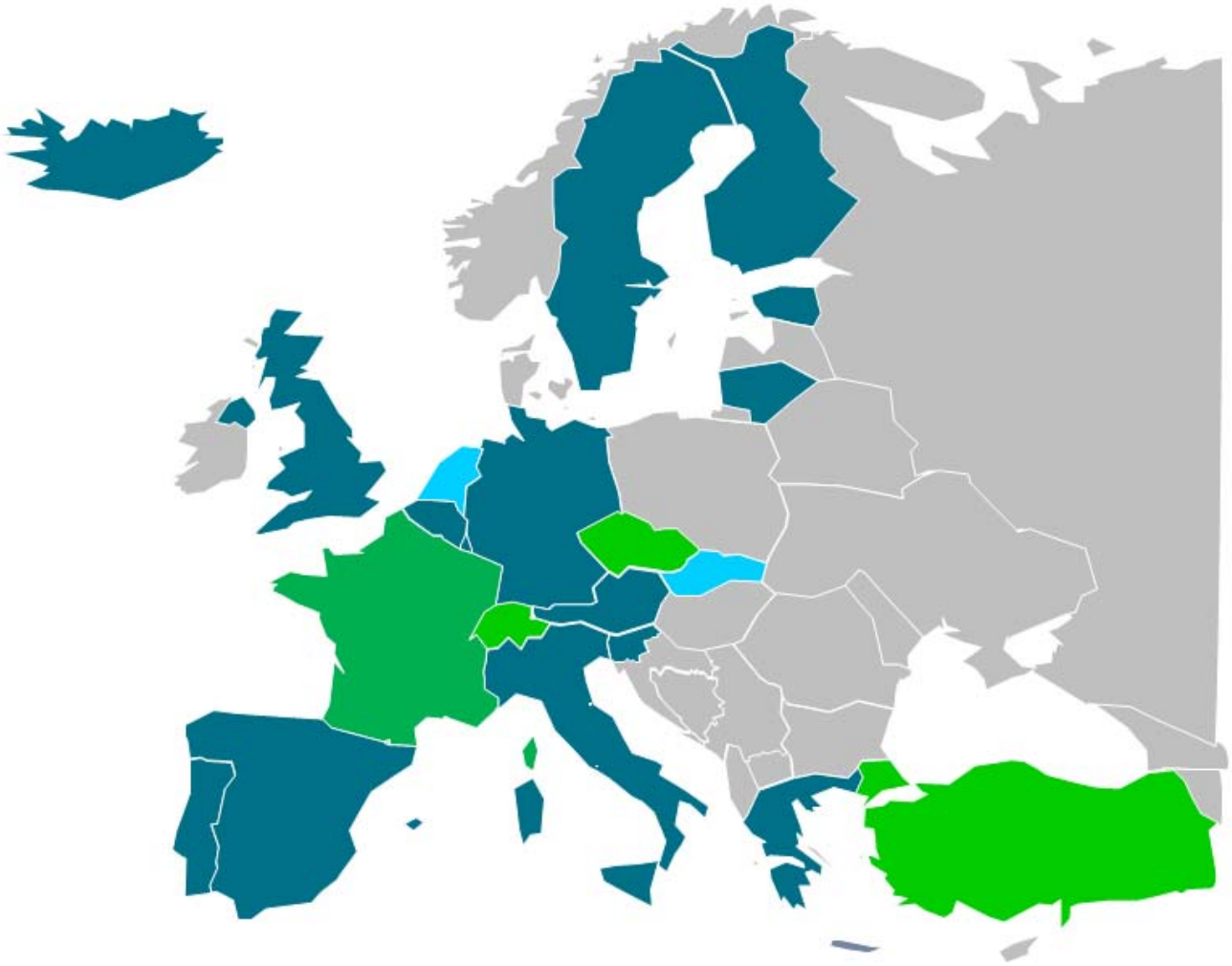
< lioy @ polito.it >

Politecnico di Torino
Dip. Automatica e Informatica

http://www.eid-stork2.eu

Stork 2.0 is a EC co-funded project
INFSO-ICT-PSP-297263

Stork (2008-2011) + Stork 2.0 (2012-2015)



21 countries

100+ e-IDs

(and much more coming as part of e-SENS)

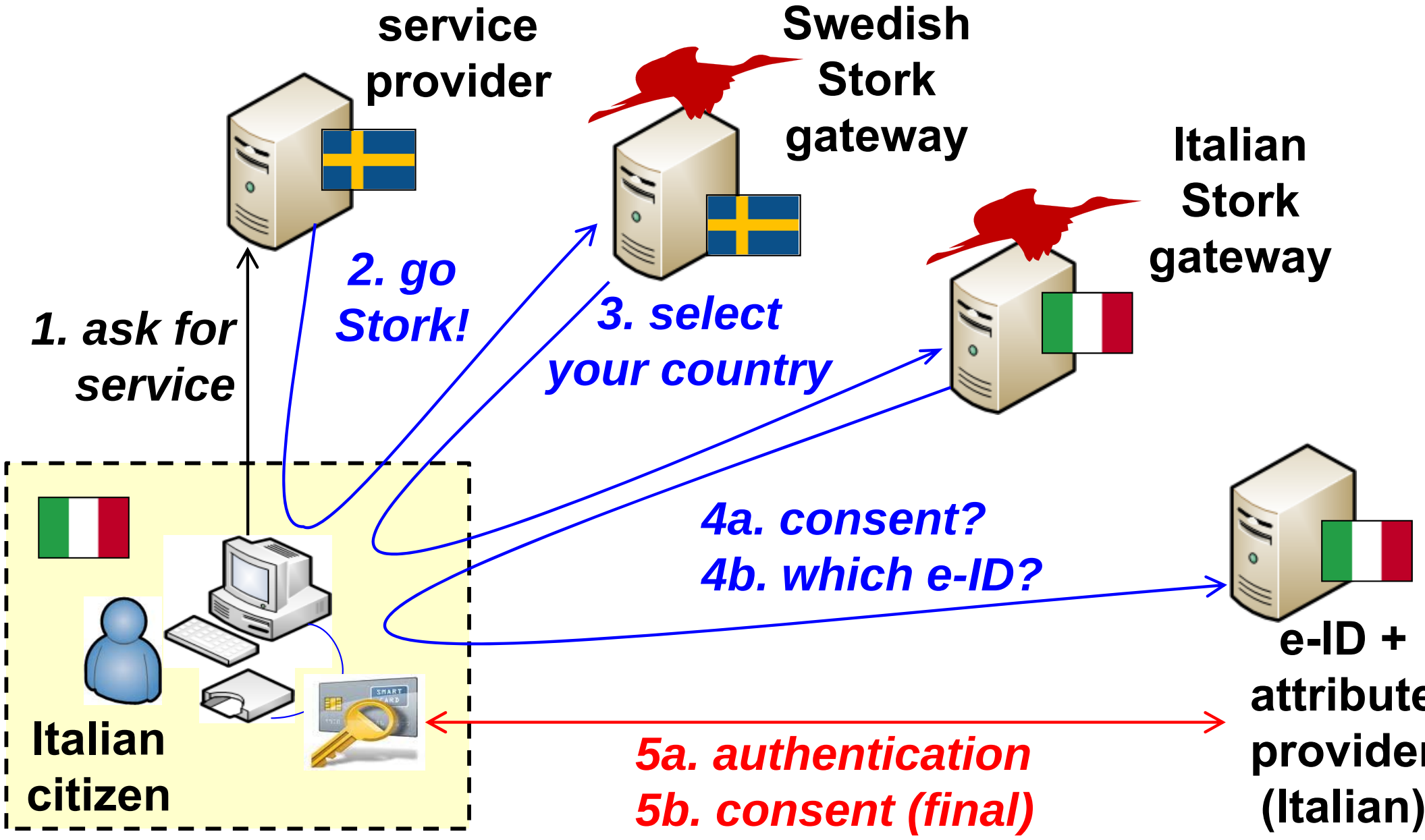
Pan-european eID

- **e-identity = authentication + certified attributes**
  - set of certified European attributes
  - lexicon (multilanguage attribute names)
  - syntax (possible values)
  - semantics (e.g. surname)
- **various authentication credentials**
  - reusable password, one-time-password, cellphone, software certificate, smart-card
  - used in a transparent way and with **legal value** (according to the citizen's country)

Adaptive security and privacy protection

- **various authentication levels**
  - crypto strength of the authentication technique
  - strength of the identification process
  - **QAA** (Quality of Authentication Assurance) 1…4
- **requested (by the service) versus effective level (depending on the authentication technique used)**
- **privacy protection and localization**
  - user talks with her own country and provides explicit consent for the required attributes
  - attributes managed end-to-end (no storage of personal data in the infrastructure)
  - minimal disclosure (NEED-TO-KNOW principle)

The Stork infrastructure



eIDAS e-ID interoperability framework (I)

- **based on the Stork architecture**
- **more alignment with standards**
  - ISO LoA (Level of Assurance)
  - use SAML native constructs where available (e.g. requested and actual LoA)
- **operational security**
  - crypto-suites for secure channels (TLS) and SAML signature/encryption – minimum and suggested
  - security management "certification"
  - trusted distribution of gateway meta-data (signature and encryption certificates, node addresses, …)
    - extended TSL or SAML meta-data

eIDAS e-ID interoperability framework (II)

- **technical improvements**
  - encryption of assertions to avoid attacks in the browser
  - gateway metadata include available attributes (to avoid asking for what is not available)
  - sector-specific gateways
  - transparent transport of sector-defined attributes

Food for thoughts

- usage of eIDAS by the private sector
- mix-and-match with other e-IDs (private or sector-specific)
- attributes, attributes and more attributes (and mandates, delagtion of powers, …)

Thank you for your attention!

www.eid-stork2.eu