Security aspects of CLIPS

Antonio Lioy

< lioy @ polito.it >

Politecnico di Torino
Dip. Automatica e Informatica

http://www.clips-project.eu/

CLIPS is an EC co-funded project
INFSO-ICT-PSP-621083

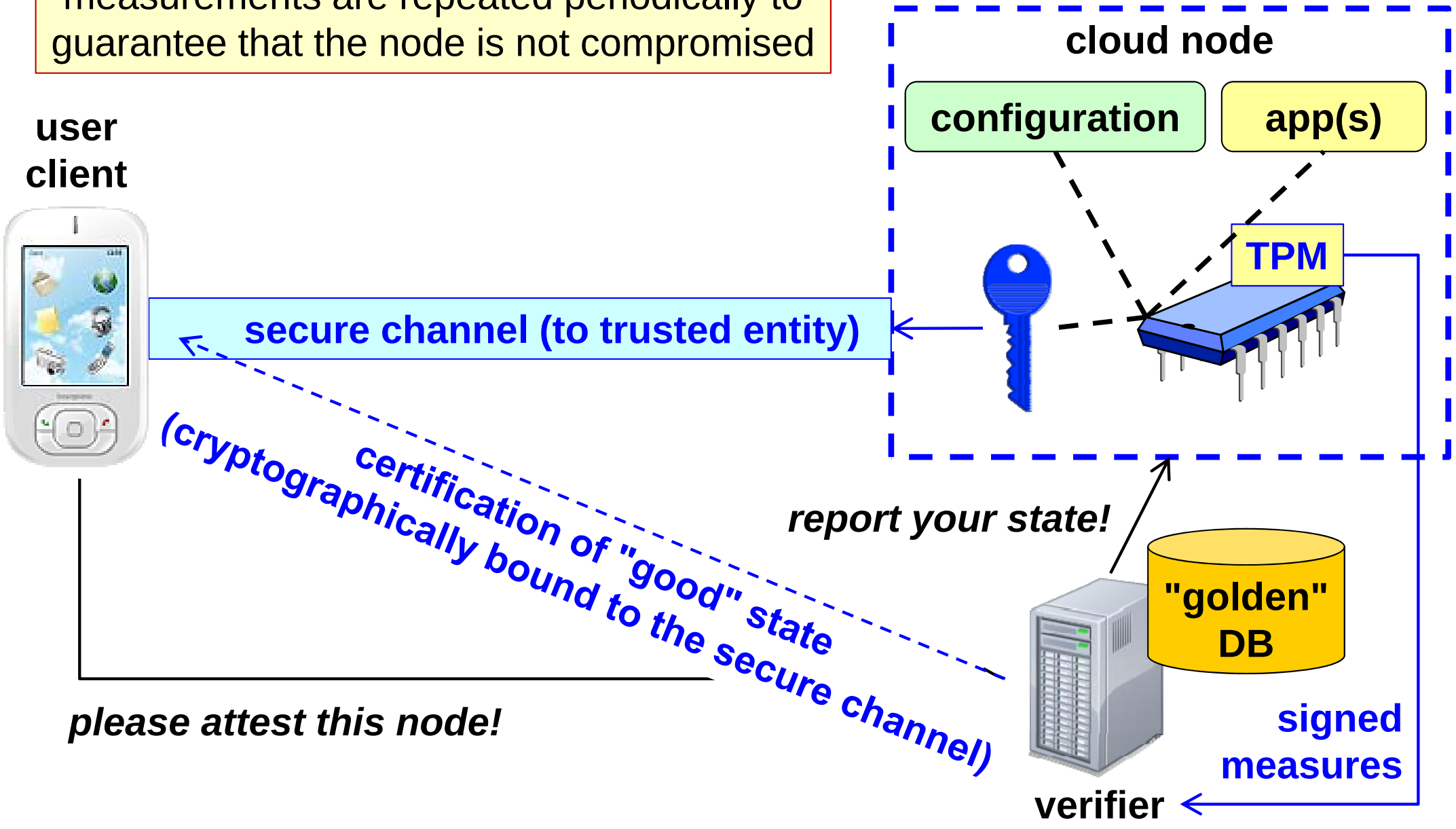
CLIPS in brief

- **CIP project (type B, grant no. 621083) feb-2014 / jul-2016**
- **coordinator: Engineering**
- **partners from Italy, Germany, Serbia, Spain, and UK**

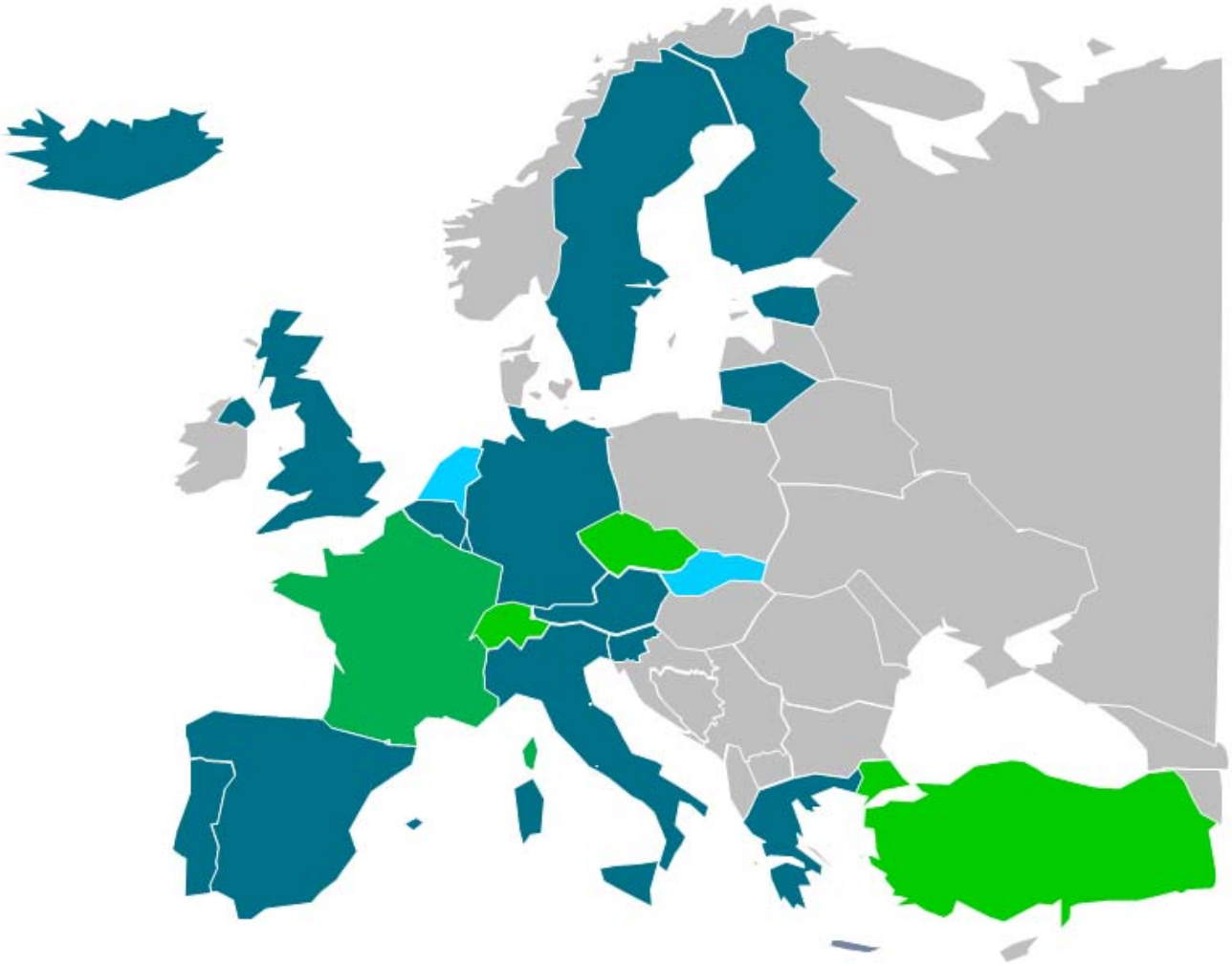
- **cloud-based platform for easy development and deployment of public administration services**
- **based on:**
  - Micro-Services = composable elementary technical services
  - Micro-Proxies = composable gateways to external services
  - a CLIPS service is a chain of Micro-Services (MS) and Micro-Proxies (MP)
- **security, trust, and privacy are critical issues**
  - e.g. confidential data remain by the P.A. that owns them

Trust in cloud nodes

measurements are repeated periodically to guarantee that the node is not compromised



European electronic identity: Stork + Stork 2.0 + e-SENS



21 countries

100+ e-IDs

(and more coming as part of e-SENS)

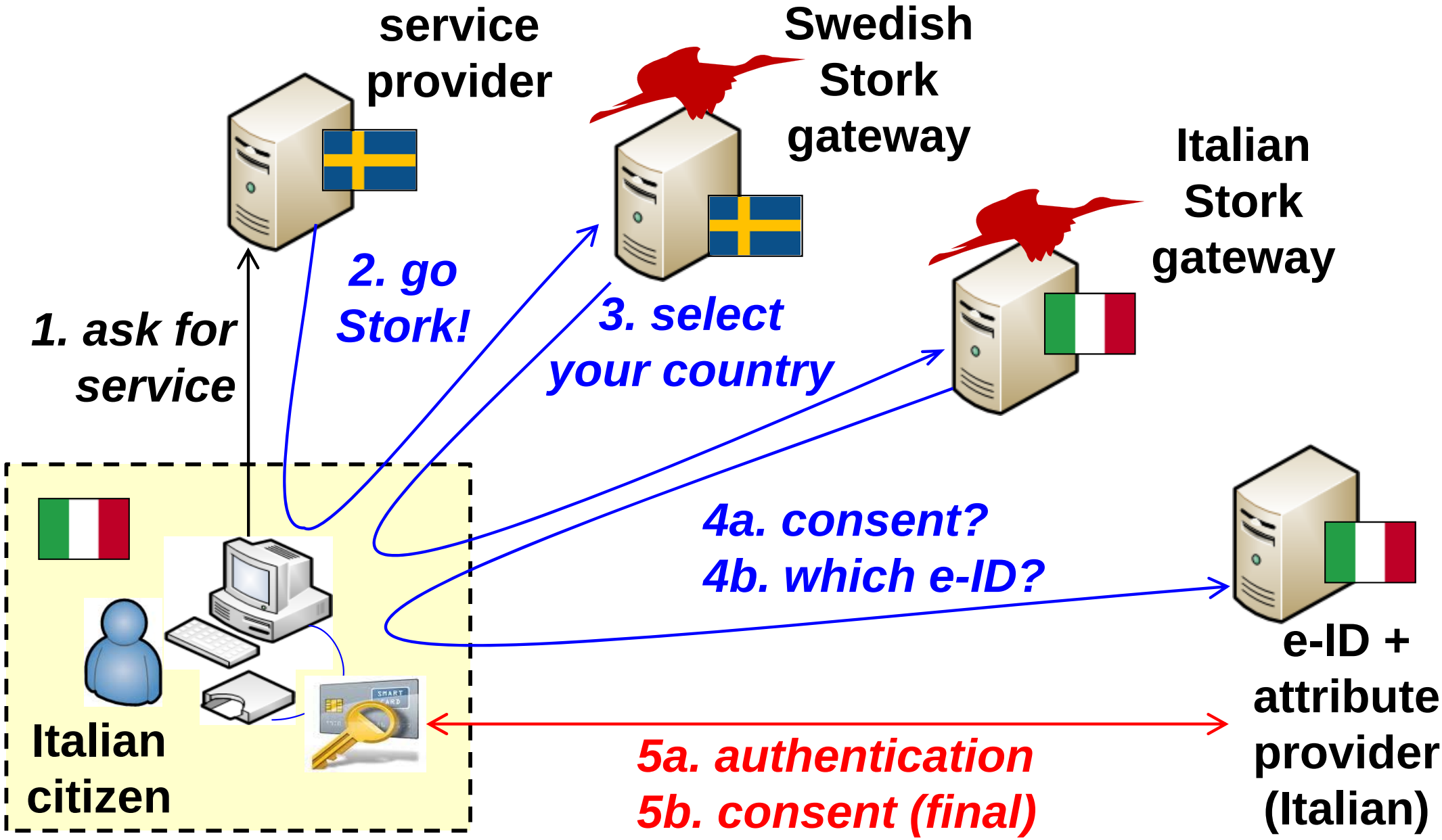
Pan-european eID

- **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

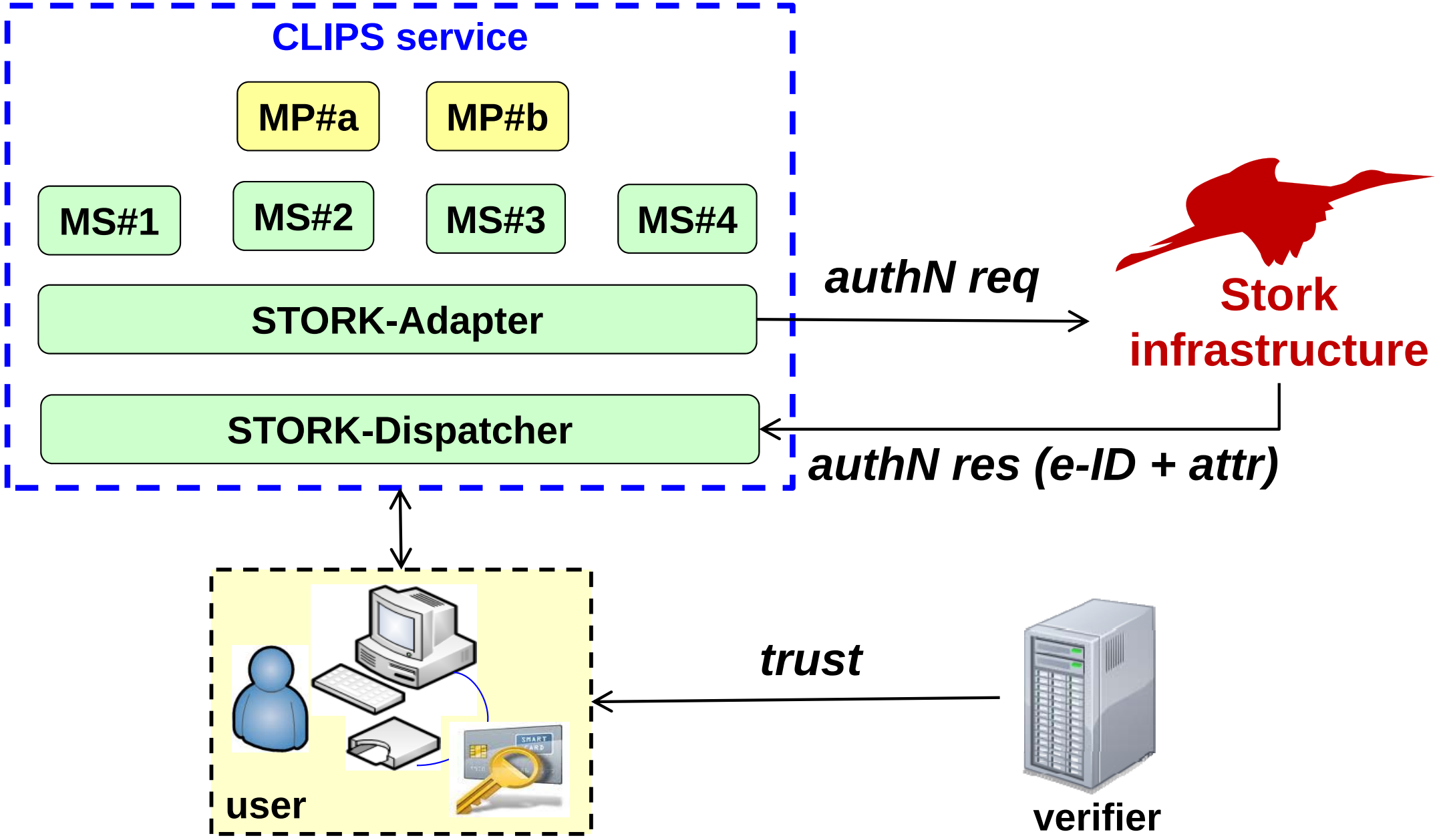
European e-ID timeline

- **STORK (2008-2011)**
  - physical person e-ID and basic attributes
- **STORK-2.0 (2012-2015)**
  - STORK + legal person e-ID, additional attributes, mandates, …
- **e-SENS (2014-2016)**
  - gateway STORK – eIDAS
- **usage of eIDAS:**
  - first nodes operational in 2016
  - mandatory for public services starting on 2018
  - optional (but welcome) by the private sector

STORK integration into CLIPS

- **a CLIPS service acts as a STORK Service Provider**
- **integration based on two adapters provided as Micro-Services:**
  - STORK-Adapter
    - initializes the STORK authentication procedure
    - converts authentication requests from CLIPS to STORK
  - STORK-Dispatcher
    - verifies & parses the STORK authentication responses
    - forwards result to MS / MP (authentication + attributes)

CLIPS : trust + e-ID



Thank you for your attention!

www.clips-project.eu