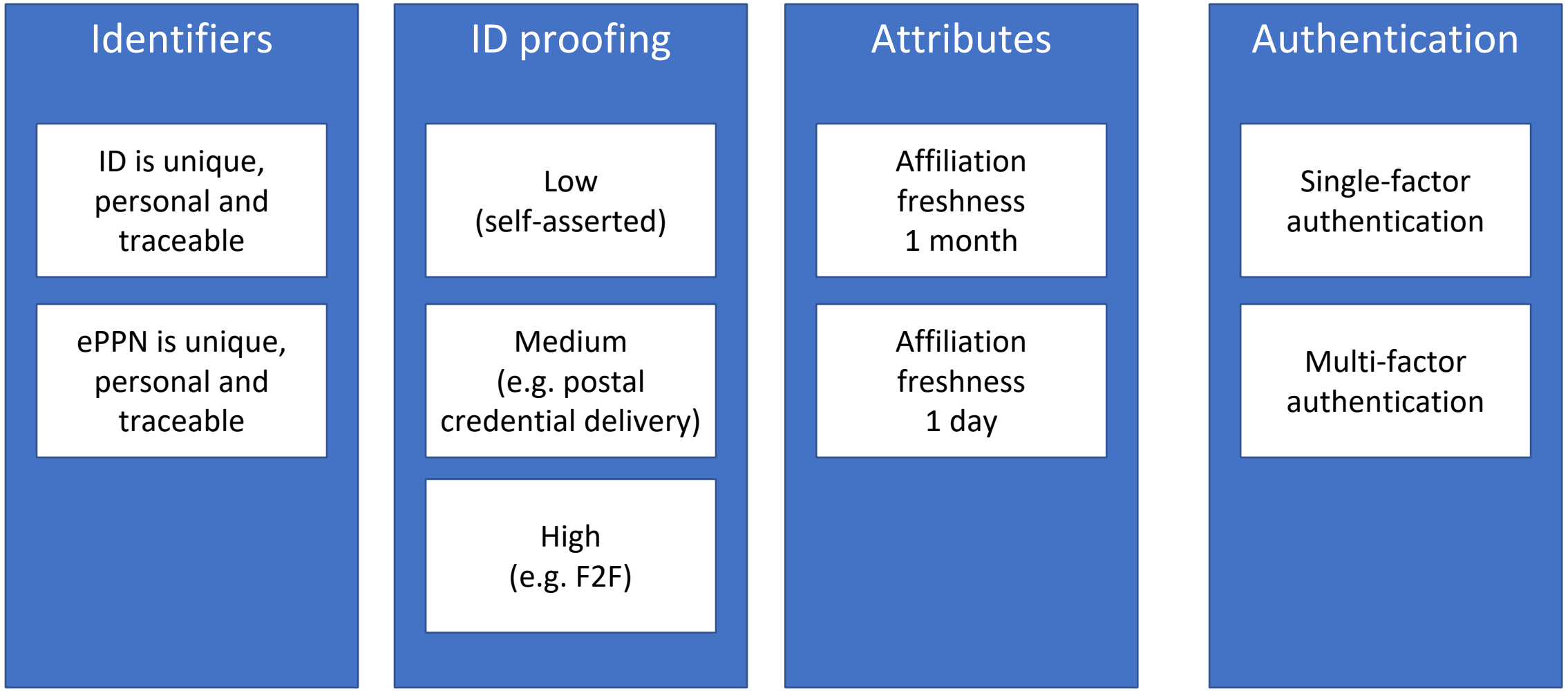
REFEDS Assurance Framework

AARC AHM 11 Apr 2018 in Athens
Mikael Linden, REFEDS assurance wg chair
mikael.linden@csc.fi

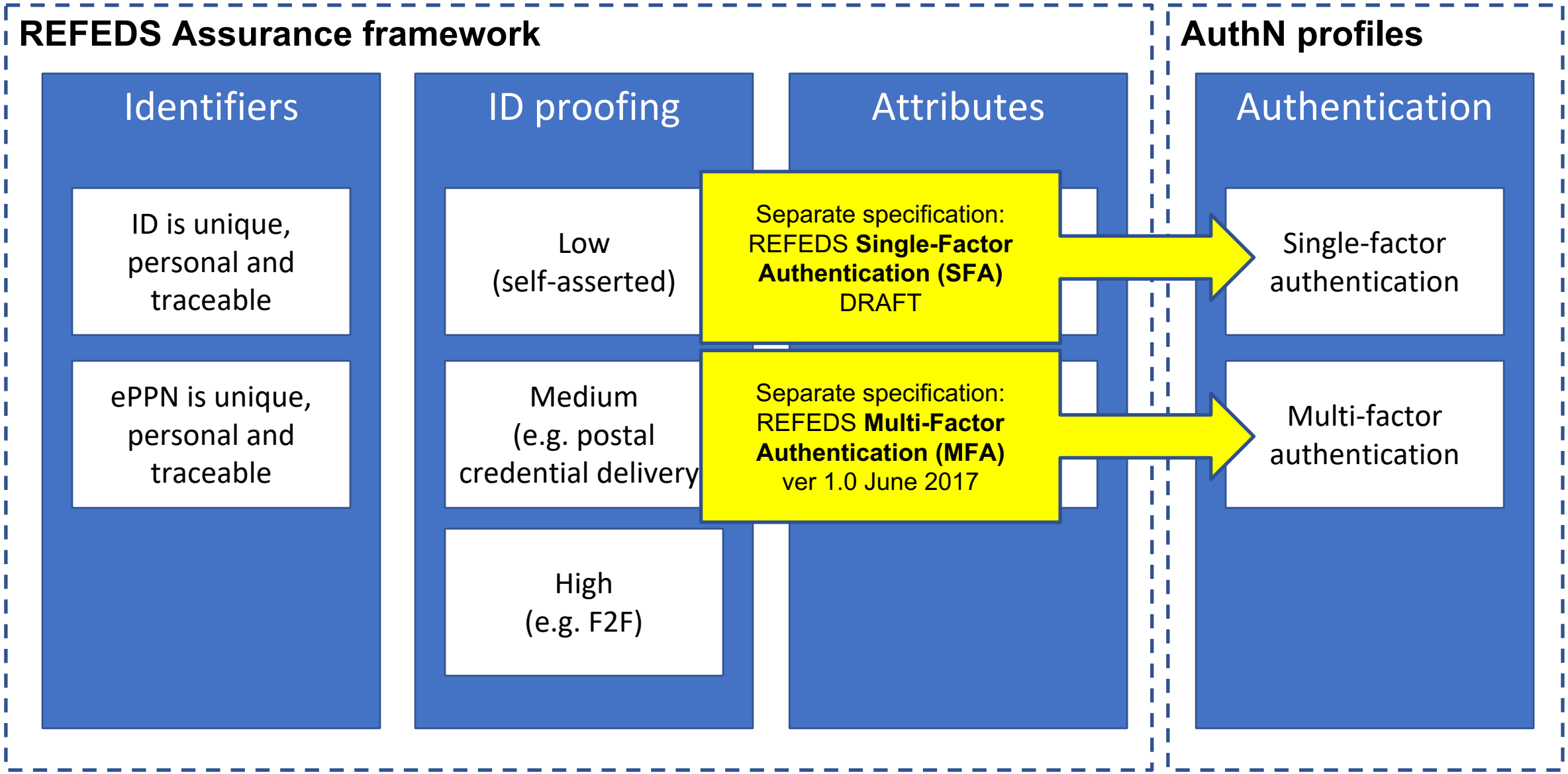
Short history and future

- 11/2015 AARC publishes minimal LoA requirements for low-risk research
- 6/2016 REFEDS establishes the Assurance working group
  - To write a specification to meet the requirements
- 4-6/2017 Public consultation on the 1st draft of the REFEDS Assurance Framework (RAF)
- Going to expose RAF to second public consultation soon
  - Together with REFEDS Single-Factor Authentication (SFA) profile
- Currently having a pilot on RAF/SFA
  - SPs: ELIXIR, BBMRI, CILogon, EGI Check-in
  - IdPs: Chicago, XCEDE, Aalto, CSC
  - Missing more IdP products (SimpleSAMLphp, ADFS, …)

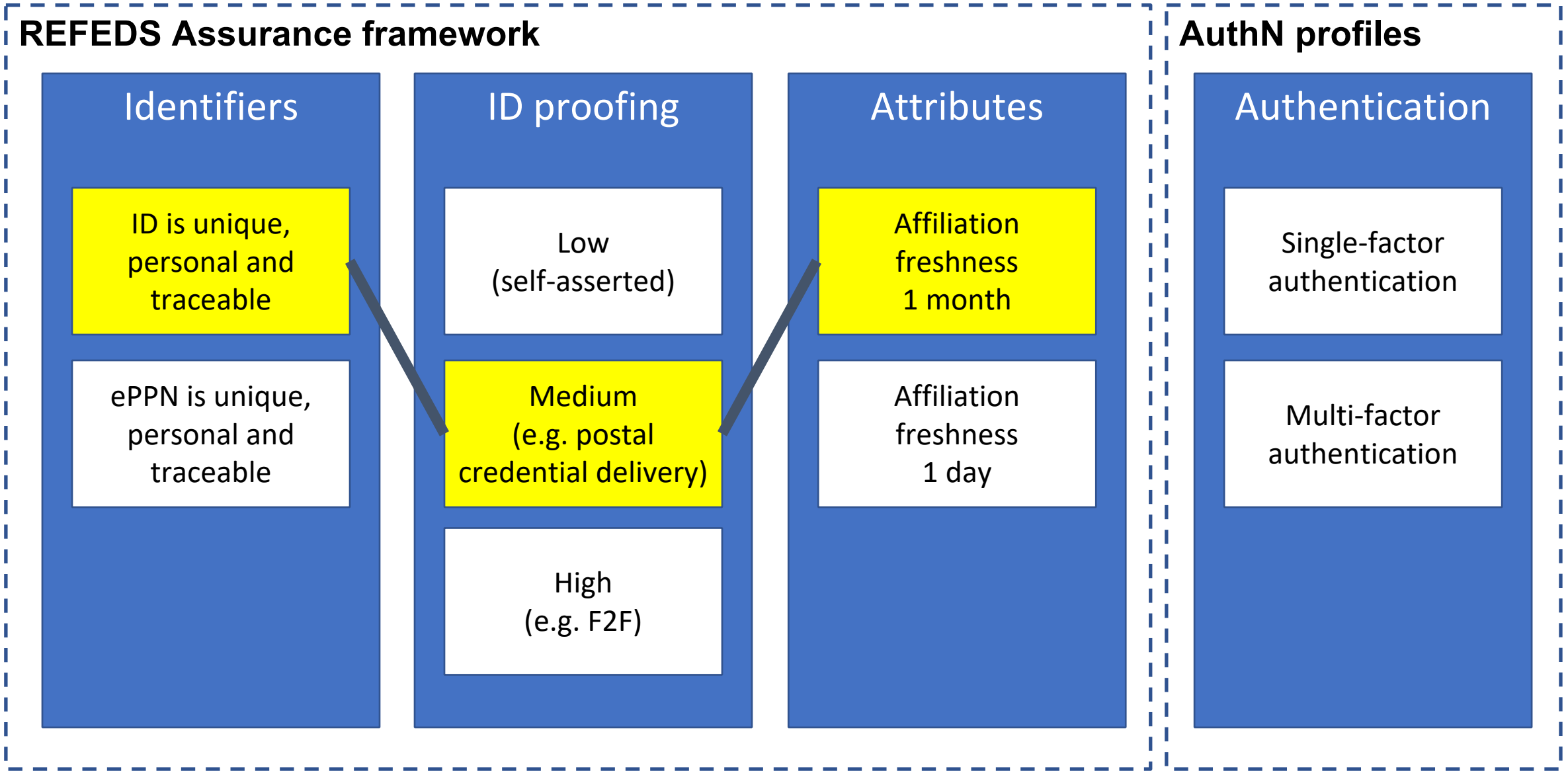
The big picture of assurance



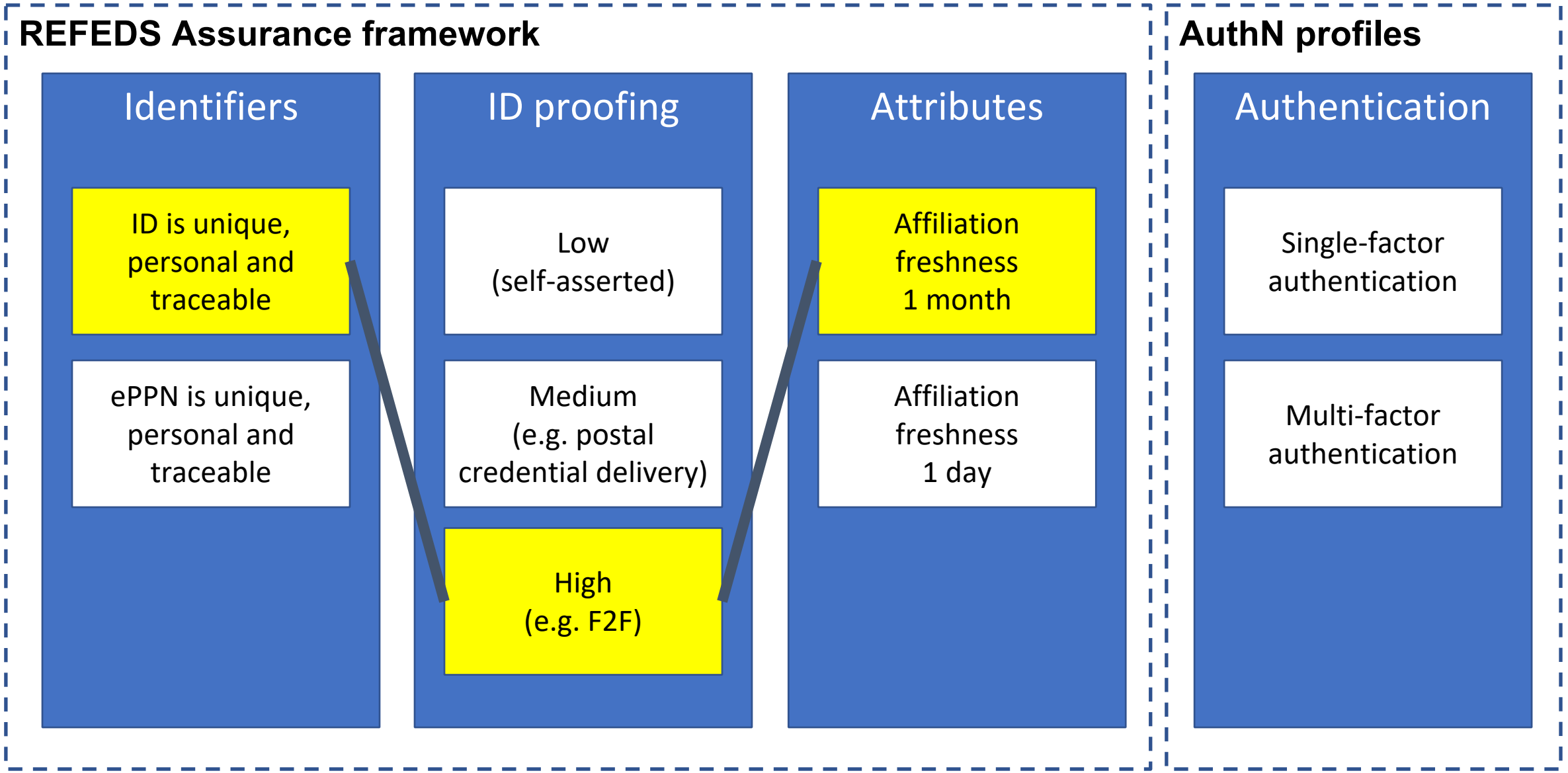
Split of responsibility clarified



“Cappuccino” for low-risk research use cases



“Espresso” for more demanding use cases



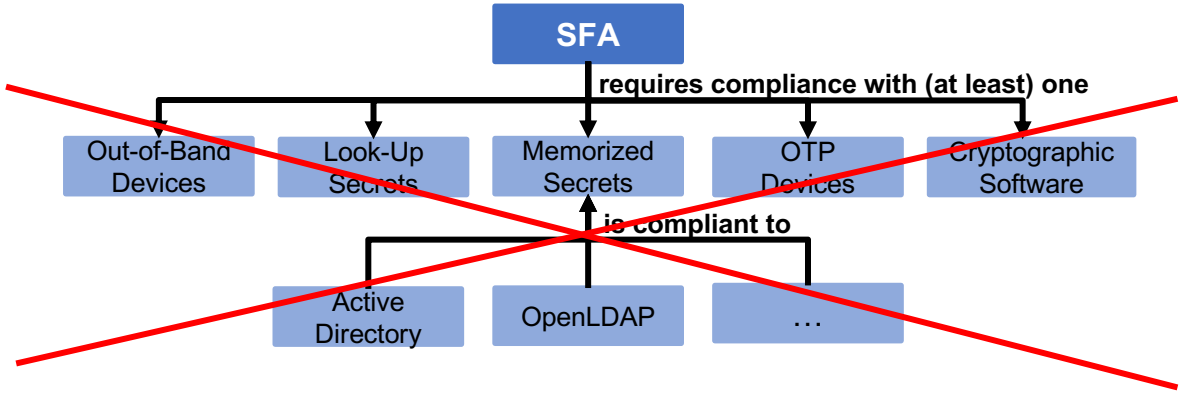
More information

- REFEDS assurance wg: https://wiki.refeds.org/x/MgDI
- mikael.linden@csc.fi

REFEDS Single-Factor Authentication Profile

- New approach: SFA v0.2
- Basic structure/hierarchy (Profile–Minimum Requirements–Recipes) dropped

  → **One** generic document covering **all** types of authentication factors



- Risk-based approach (controls) dropped

REFEDS Single-Factor Authentication Profile

- SAML and OIDC authentication context
- Terminology used in this document based on NIST 800-63B
- Defines a security baseline for AuthN using a single factor
- Two main criteria:
    1) Requirements for authentication factors
        - Properties of the factor itself:
            Minimum secret length, Basis for secret generation
        - Threat protection:
            Prevent online guessing, Protect the secret cryptographically
    2) Requirements for replacement of a lost authentication factor