A-SIT

A-SIT Plus GmbH

Austrian E-ID 2020
Overview, Discussion

Peter Teufl, peter.teufl@a-sit.at

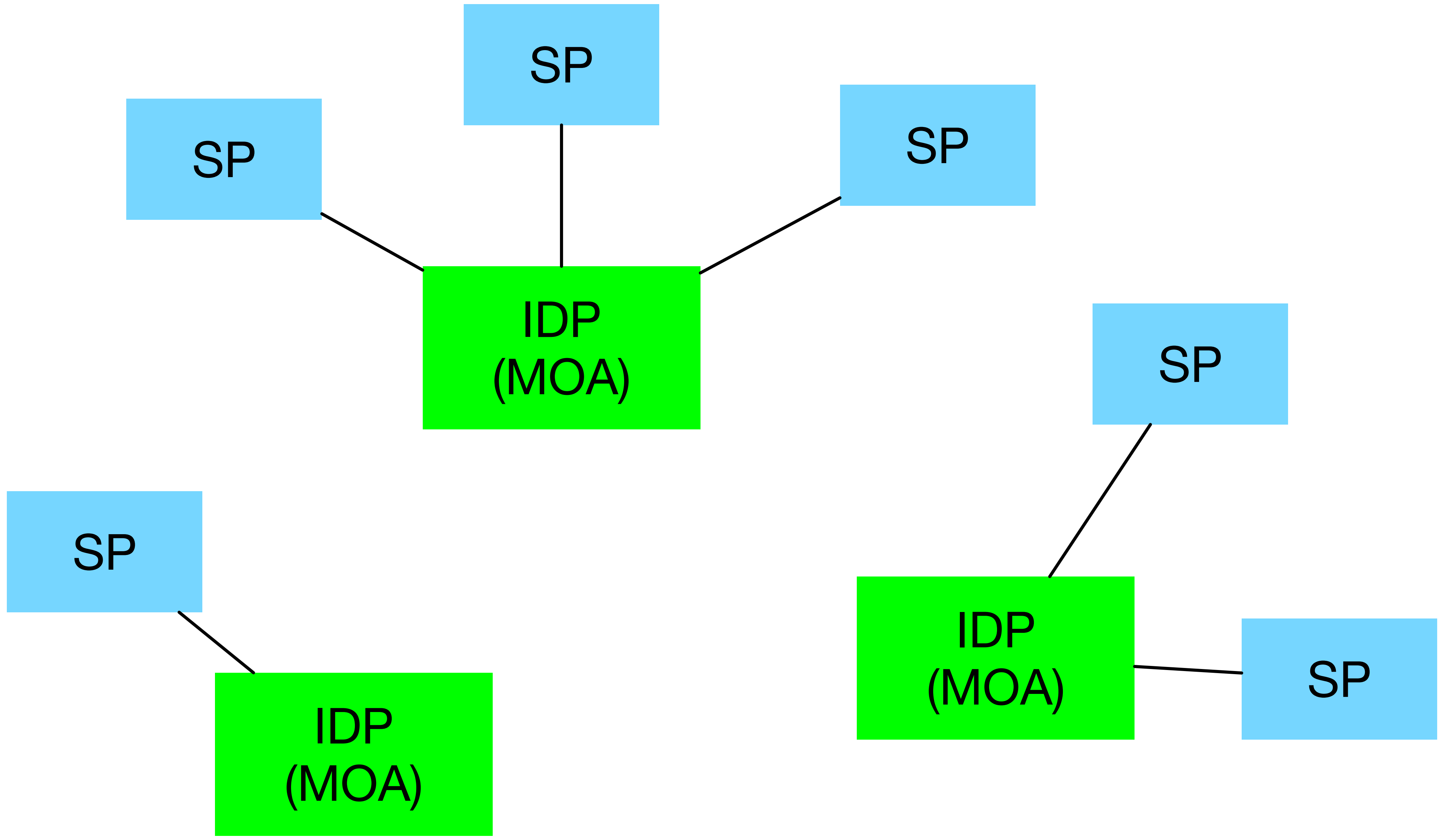
SEED TOPICS FOR DISCUSSIONS

- Planned E-ID solution for Austria
  - Compared to current solution
- Authentication, Security
- Mobile challenges

A-SIT Plus GmbH

CURRENT SOLUTION

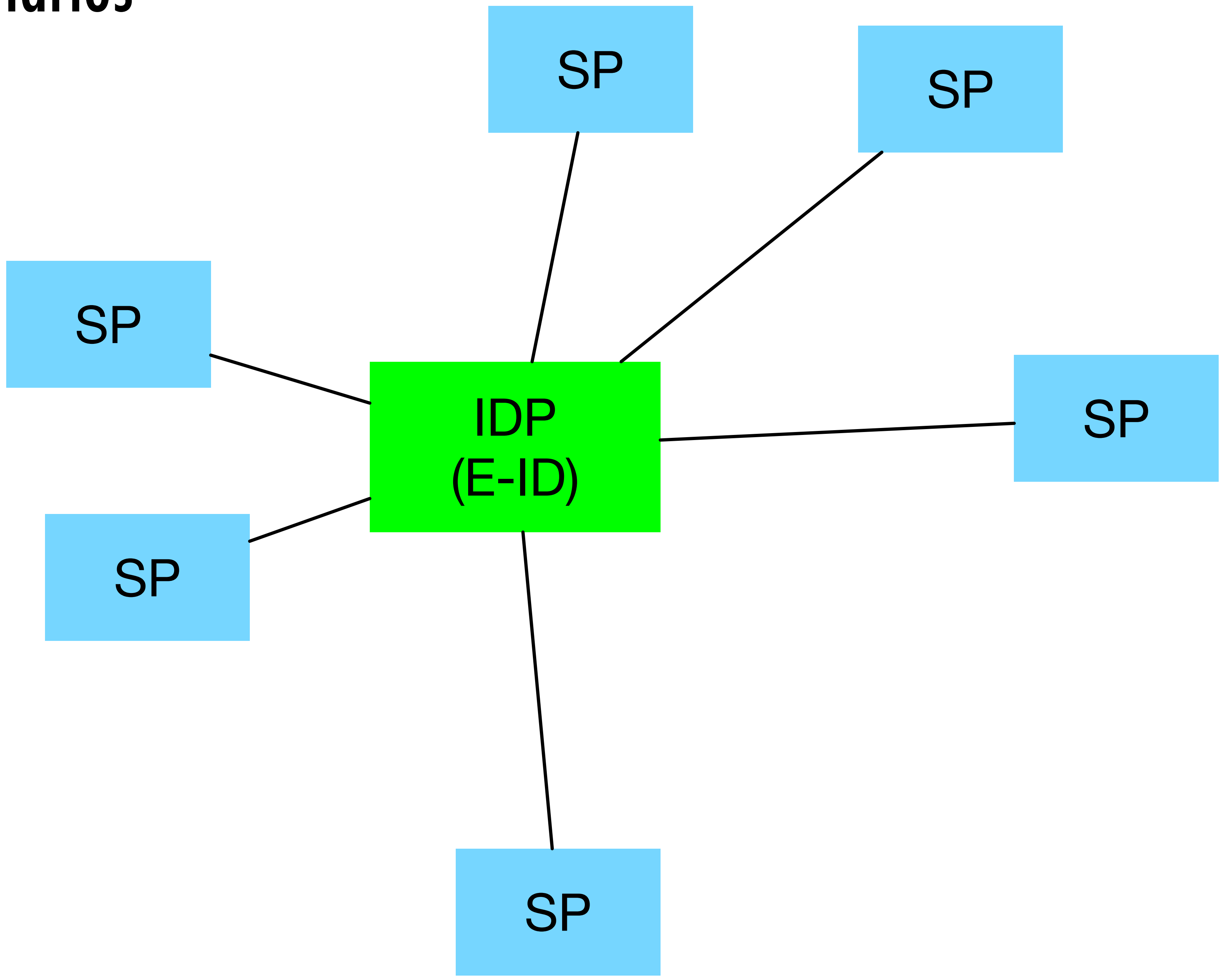
- De-central solution
  - single service provider or groups of service providers set up their own IDP (MOA)
- Authentication
  - qualified signature, Chip card or mobile phone signature (HandySignatur, remote qualified signature)
- Attributes
  - “minimum dataset”: sector specific ID, name, date-of-birth
  - stored on the chip-card and/or mobile phone signature (issued and signed by authority)
  - mandates
- Web-only
- Registration
  - multiple paths: FinanzOnline, wide range of ROs



A-SIT Plus GmbH

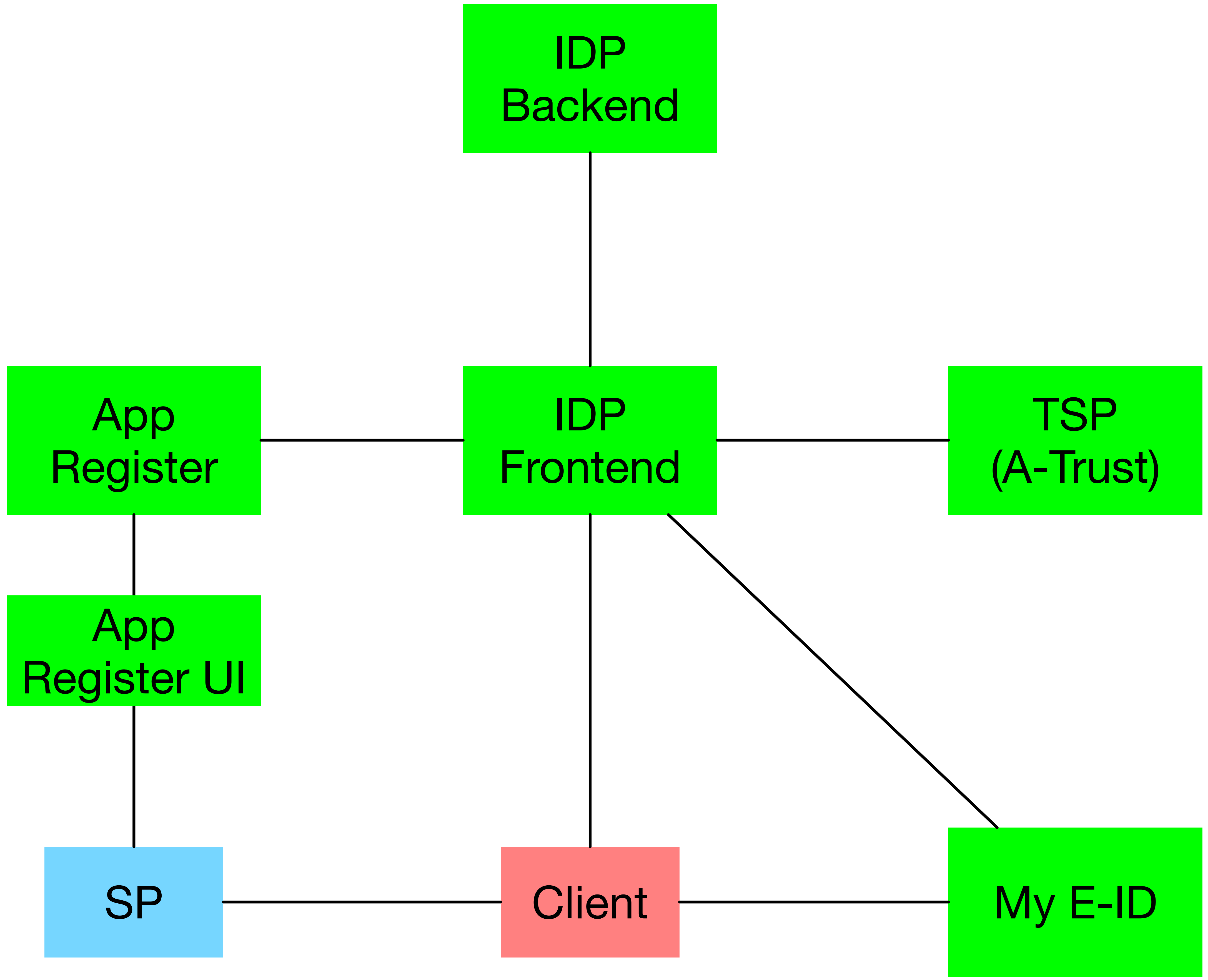
E-ID 2020

- **Central solution**
  - a single IDP will be created to lower SP burden, provide new features
  - Plug-ins for legacy systems, which help the SPs within the transition phase
- **Authentication**
  - primary focus: mobile-phone-signature and additional mechanisms for mobile scenarios
- **Attributes**
  - "minimum dataset": sector specific ID, name, date-of-birth
  - plans for additional attributes (address, driving licence ID, etc.)
  - issued/signed by authority, during each logon-procedure
  - mandates
- **Web (SAML, OIDC) and mobile (OIDC)**
- **Registration**
  - passport office, one-time visit (E-ID full)
  - simplified upgrade (E-ID light) from existing mobile-phone-signature users (time-limit, then passport office)



E-ID 2020 - ZOOM IN

- TSP
  - for mobile phone signature authentication
- IDP Backend
  - issuing attributes, signing of issued attributes
- IDP Frontend
  - IDP protocols (SAML, OIDC)
- App Register and UI
  - Central registry for service providers (self-registration with manual accreditation process)
    - SAML/OIDC metadata, friendly names, data protection policies etc.
- My E-ID
  - device management, data protection inquiries, recovery, revocation etc.



A-SIT Plus GmbH

TIMEFRAME

- Pilot operation very soon
  - dual operation of old/new solution
  - gradual shift for service providers
- Complete switch to new system after adequate pilot-time
- Digitale Amt app, will then be upgraded to E-ID app

A-SIT
A-SIT Plus GmbH

E-ID 2020 - AUTHENTICATION

- Mobile phone signature
  - 3 factors
    - <u>knowledge</u> (password) verified by server
    - <u>possession</u>: asymmetric key in trust-zone of smartphone
      (Secure Enclave for Apple, different solutions for Android phones)
    - <u>inherence</u>: Fingerprint, Face-ID (depended on the phone, but in general iris scans, 3d-face scans, simple face recognition via photo not accepted), for creating a signature with the key stored in the trust-zone
- Continuation, only possible on the same device
  - for mobile apps:
    - service provider decides on max time frame
    - mobile phone signature must have been used within this time-frame
      - then, simpler authentication with 2 factors (<u>possession</u>, <u>inherence</u>)

A-SIT Plus GmbH

E-ID 2020 - AUTHENTICATION

- Continuation
  - Asymmetric key is bound to mobile phone signature creation
  - signed record is bound to the asymmetric key and the current device
  - Why:
    - in mobile use cases we often require quick subsequent authentication procedures by the user
      - e.g. as seen in banking apps
      - usability and security: entering the mobile phone signature password for every auth procedure is problematic (usability, and security due to mobile environment)
    - E-ID system provides the means, so that service providers don’t need to focus on authentication but are able to rely on the E-ID system

E-ID 2020 - SECURITY

- General perspective
  - detailed risk analysis of all technical/org. processes
  - external audits/pen-testing
  - overall ISMS for the involved entities
  - detailed incident handling procedures
- Technical perspective
  - Cryptographic keys within hardware-security-modules
    (SAML, OIDC keys but also temporary keys required during authentication procedures)
  - HSM facades for rapidly creating testing, production environments with the appropriate keys and trust-relations
  - Cryptographic links between essential operations (e.g. continued authentication linked to mobile phone signature)
  - New mobile phone capabilities: key attestation, trust-zones etc.
  - Root-detection with standard-means and key attestation

E-ID 2020 - MOBILE STORIES

- Continuous challenges
  - major operating system versions: significant changes
  - Android
    - diversity of providers, Google specifications not met
    - Samsung, Huawei devices required specific solutions (documented procedures not working)
    - continuous evolution of features (e.g. face ID on Pixel 4, new APIs which e.g. break dialogs on other phones, e.g. OnePlus)
    - key attestation not correctly implemented by various providers
    - testing on device clouds and many physical devices is essential
  - IOS
    - very small diversity, still significant changes also during non-major updates