deutsches forschungsnetz

IdP Hosting

Shibboleth/Federation Operator Tutorial (TIIME 2018) | 6. Feb. 2018

Wolfgang Pempe

What is an IdP and how to operate it?

An Identity Provider (IdP) is…

- … a piece of software on top of a user directory / IDM system
- … a connector speaking SAML to the outside world, i.e. SPs
- … an authentication service
  - user credentials are not exposed to an SP (“Relying Party”)
- … an attribute provider (usually)
  - reads ‘raw’ attributes from user directory, generates new attributes in dependency of existing ones (e.g. ePSA) and turns them into SP-readable objects

When operating an IdP you'd have to …

- … understand how it works, especially
  - how attributes are generated, released and transferred
  - how Persistent Name IDs are generated, stored and what impact eventual configuration changes would have
- … apply software and/or security updates on a (more or less) regular basis
  - … not only for the IdP itself but for the whole system environment
  - keep in mind that people enter their passwords (or any other credentials) there!
- … be aware of data protection issues and regulations
  - user information and consent
  - data minimization (→ attribute release)

So what about hosting?

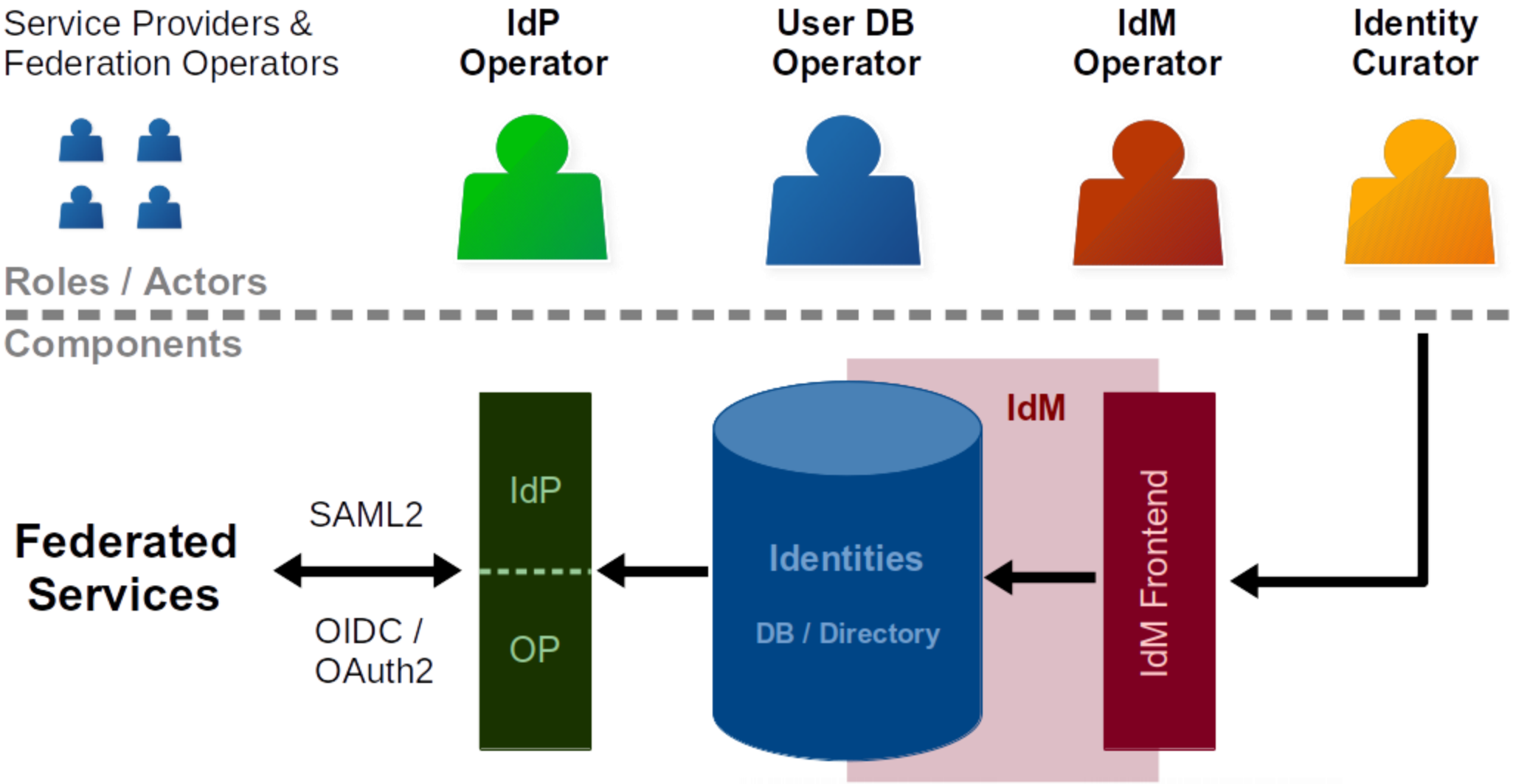
- Find a reliable partner for hosting an IdP …
  - Cost model?
  - Sustainability?
  - Court of jurisdiction? (→ data protection etc.)
- Data protection and security
  - People enter their user credentials at the IdP
  - IdP operator has access to user data
  - Depending on the contractual model, users have to be informed that their data is processed by a third party (data controller vs. data processor)
- Well-established solutions and providers are available, federations as well as commercial companies

Some Caveats…

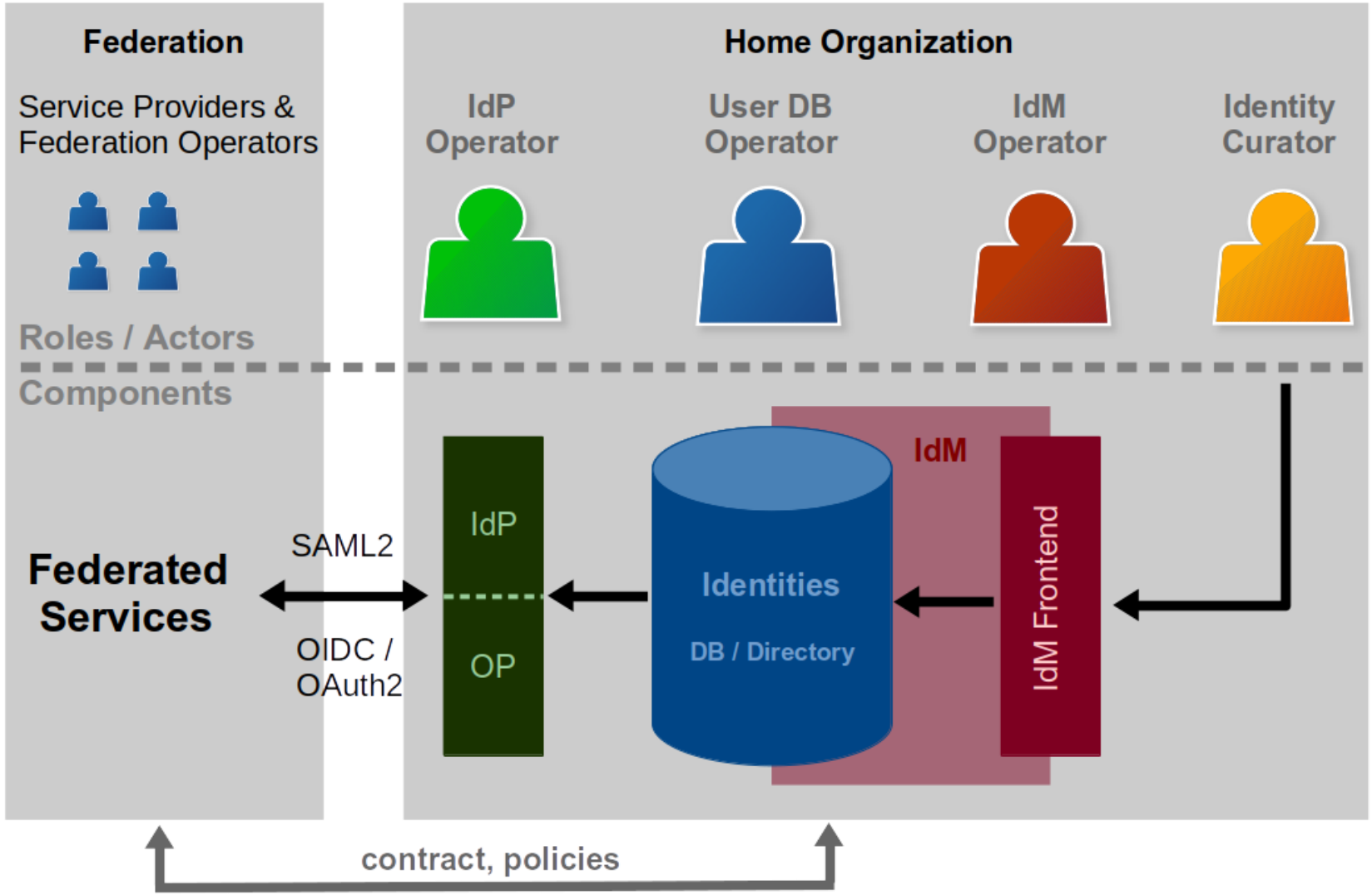
- **No shipping of private keys**
  - The hosting provider is responsible for generating keys and CSRs, esp. for Webserver TLS
- Home Organization is responsible for **DNS** entries, but hosting provider for backwards resolution
- **Access to user directory:**
  - Home Org. has to open up (and keep open!) the relevant (LDAP) ports and provide a service user in order to enable the IdP to perform the necessary bind operations
  - No unannounced key/cert rollovers on the LDAP interface!
- **Identify the contact person(s)** at the Home Organization who is/are entitled to submit change requests, in particular wrt. attribute release
- Agree on a **support model** for end users beforehand(!)

Scenarios for IdP Hosting

Components and Roles

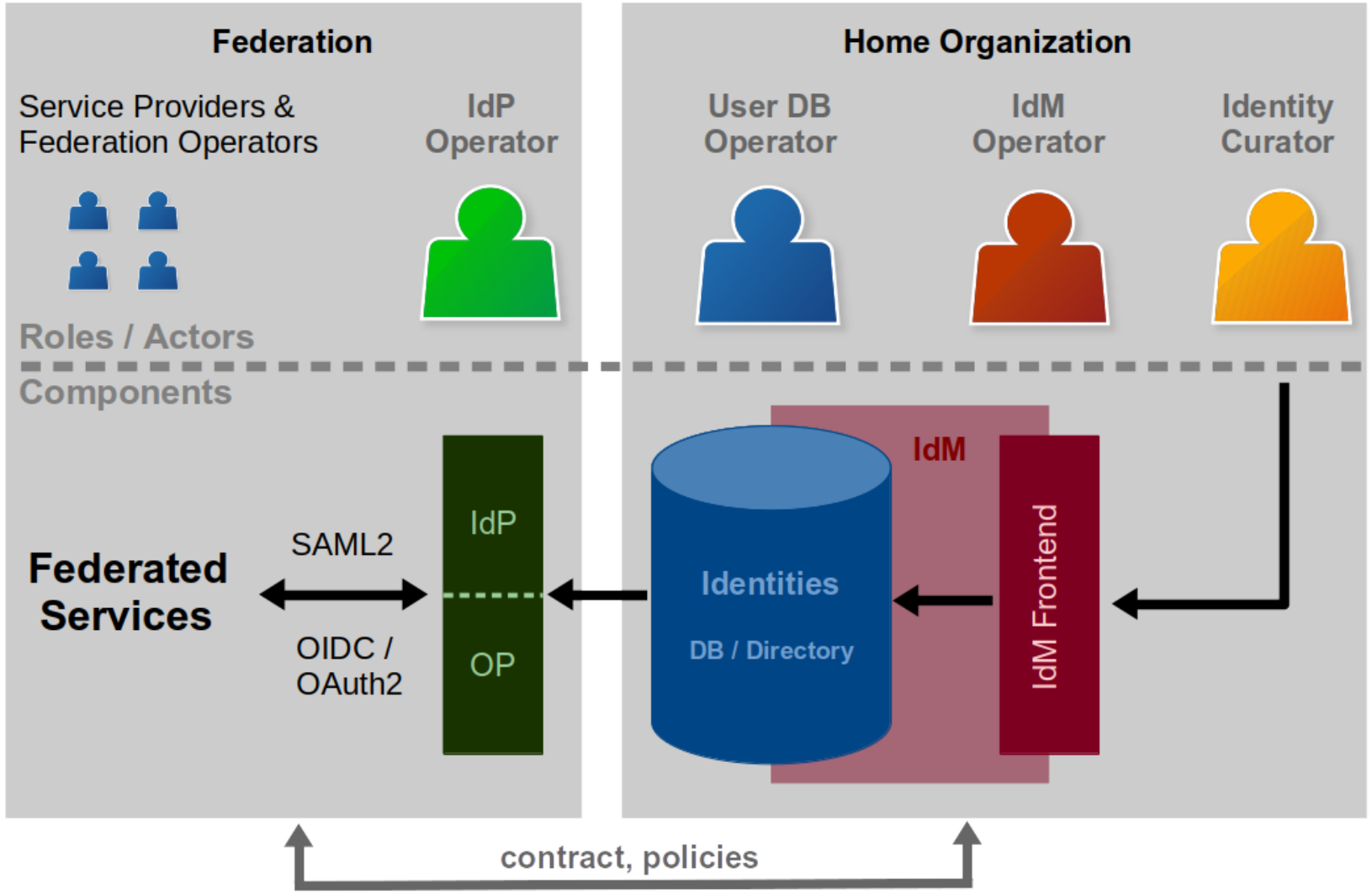


The Standard Model



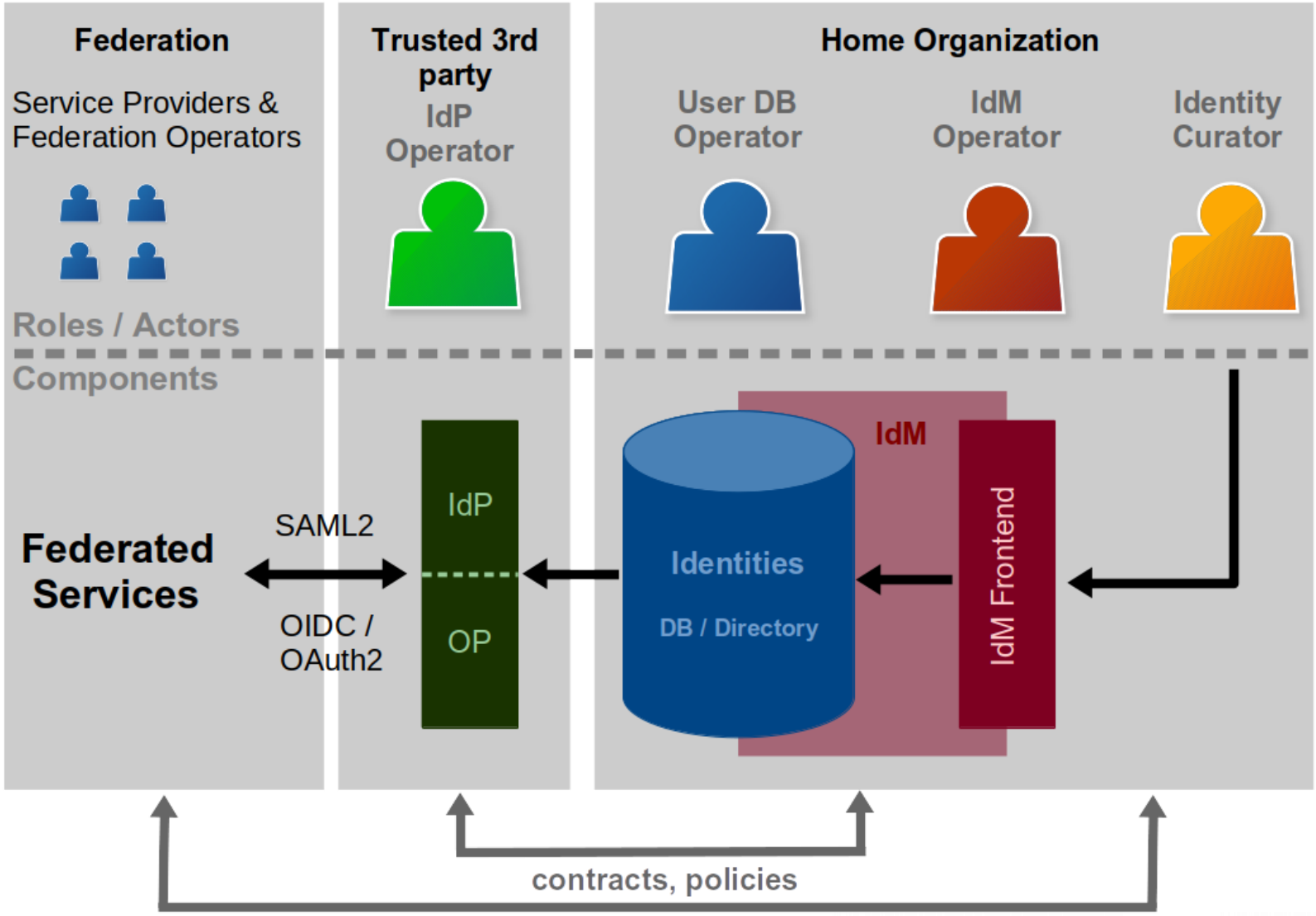
- The Home Organization does everything itself
- Most universities and larger research institutes choose this model
- Difficult for smaller institutions, where the whole IT infrastructure is operated by 2 or 3 persons…

IdP Hosted by Federation Operator



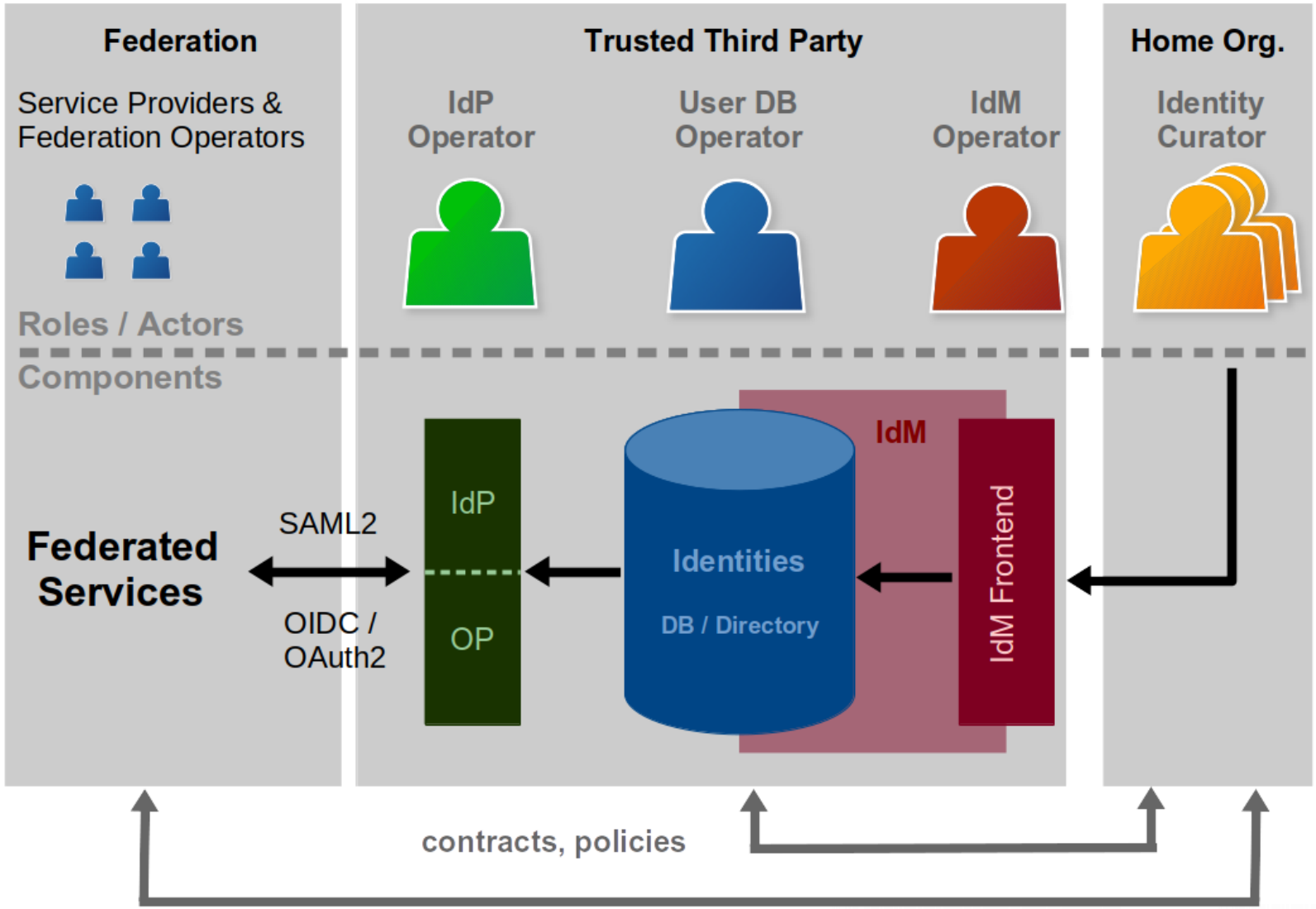
- Some federations offer this kind of service, e.g. SWITCHaai (DFN-AAI no longer)
- In a Hub-and-Spoke model like the Norwegian one, the federation operates one single IdP to which the user directories of all Home Orgs are connected

IdP Hosted by Trusted 3rd Party



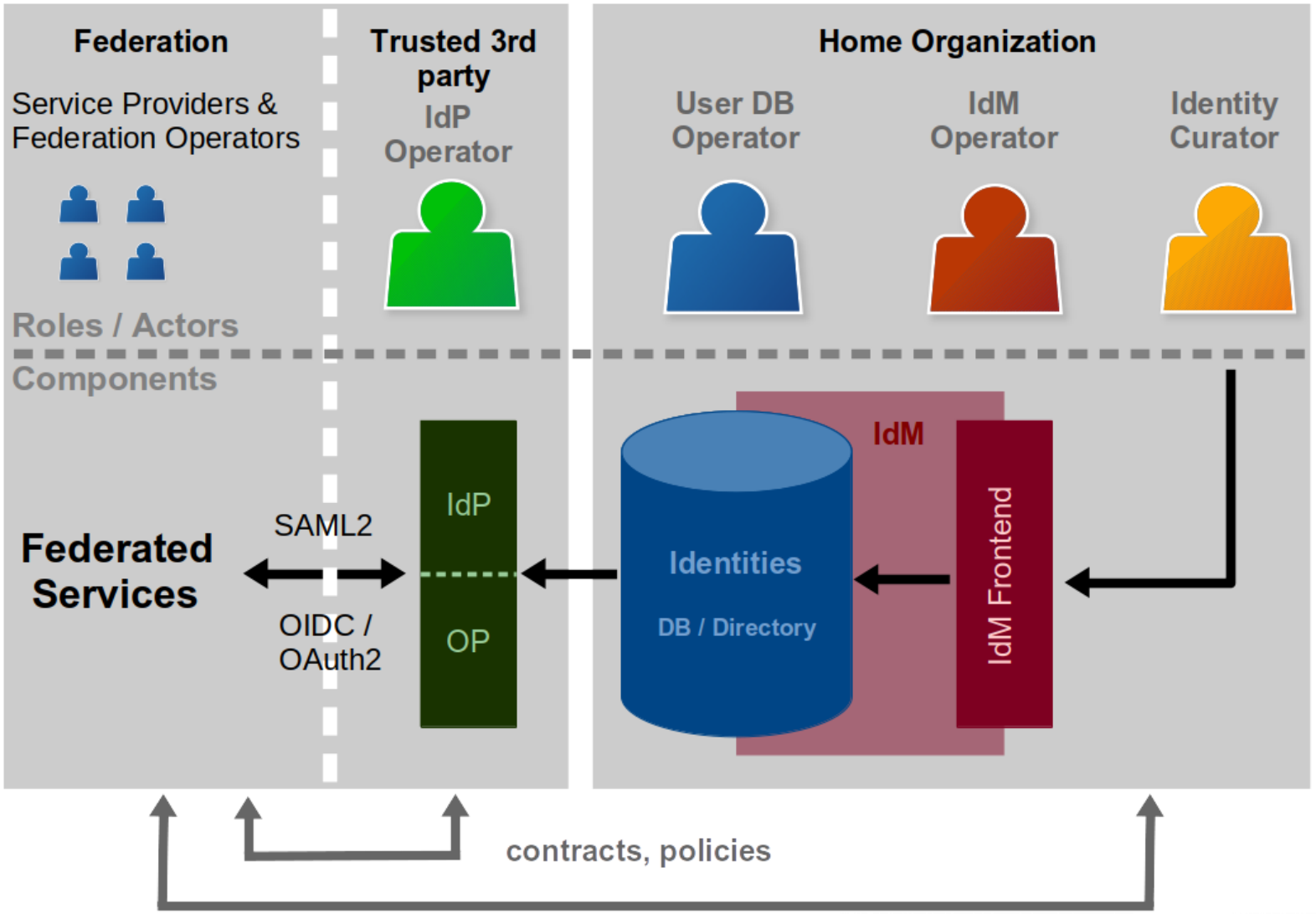
- The Home Org delegates the task of operating the IdP to a (trusted) third party, usually a commercial provider
- Contractual relationship between Home Org and provider
- Transparent for the federation operator

IdP **and** IDM Hosted by Trusted 3rd Party



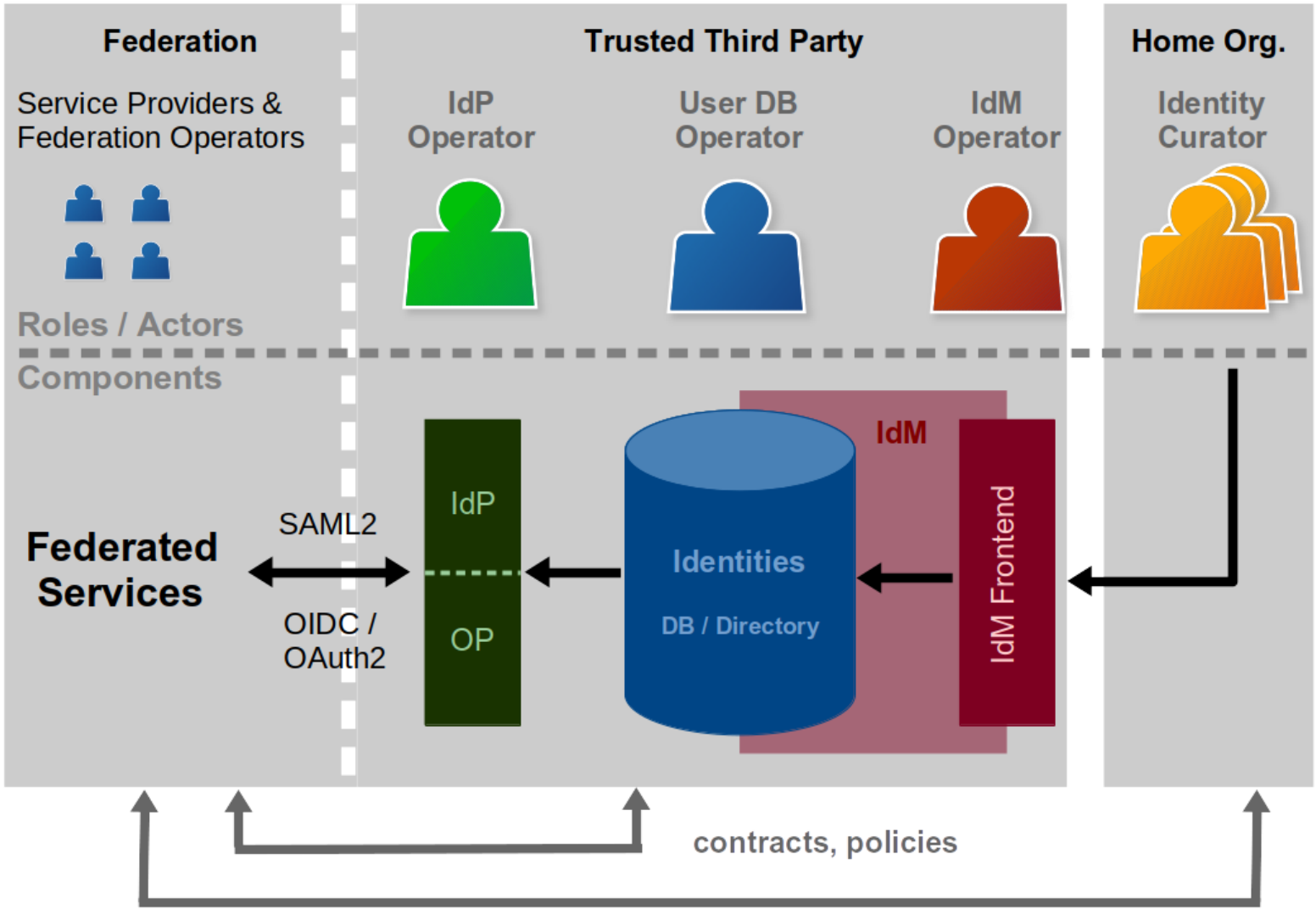
- The Home Org delegates also the operating the IDM system to a (trusted) third party, usually a commercial provider (eg. https://samlidp.io)
- User management, provisioning (and de-provisioning!) of users must be carried out by the Home Organization
- Only an option for very small institutions

IdP Hosted on Behalf of Federation Operator



- The federation delegates the task of operating IdPs (or all technical components of its infrastructure) to a (trusted) third party, maybe a commercial provider
- Contractual relationship between federation and provider
- Transparent for the Home Organizations

IdP **and** IDM Hosted on Behalf of FedOp



- The federation delegates the task of operating IdPs + IDM (or all technical components of its infrastructure) to a (trusted) third party, maybe a commercial provider
- Contractual relationship between federation and provider
- Transparent for the Home Organizations

Any Questions, Comments?

- Contact
  - Wolfgang Pempe

Email: pempe@dfn.de
Phone: +49-30-884299-9124
Fax: +49-30-884299-370

Address:
DFN-Verein, Geschäftsstelle
Alexanderplatz 1
D-10178 Berlin

Germany