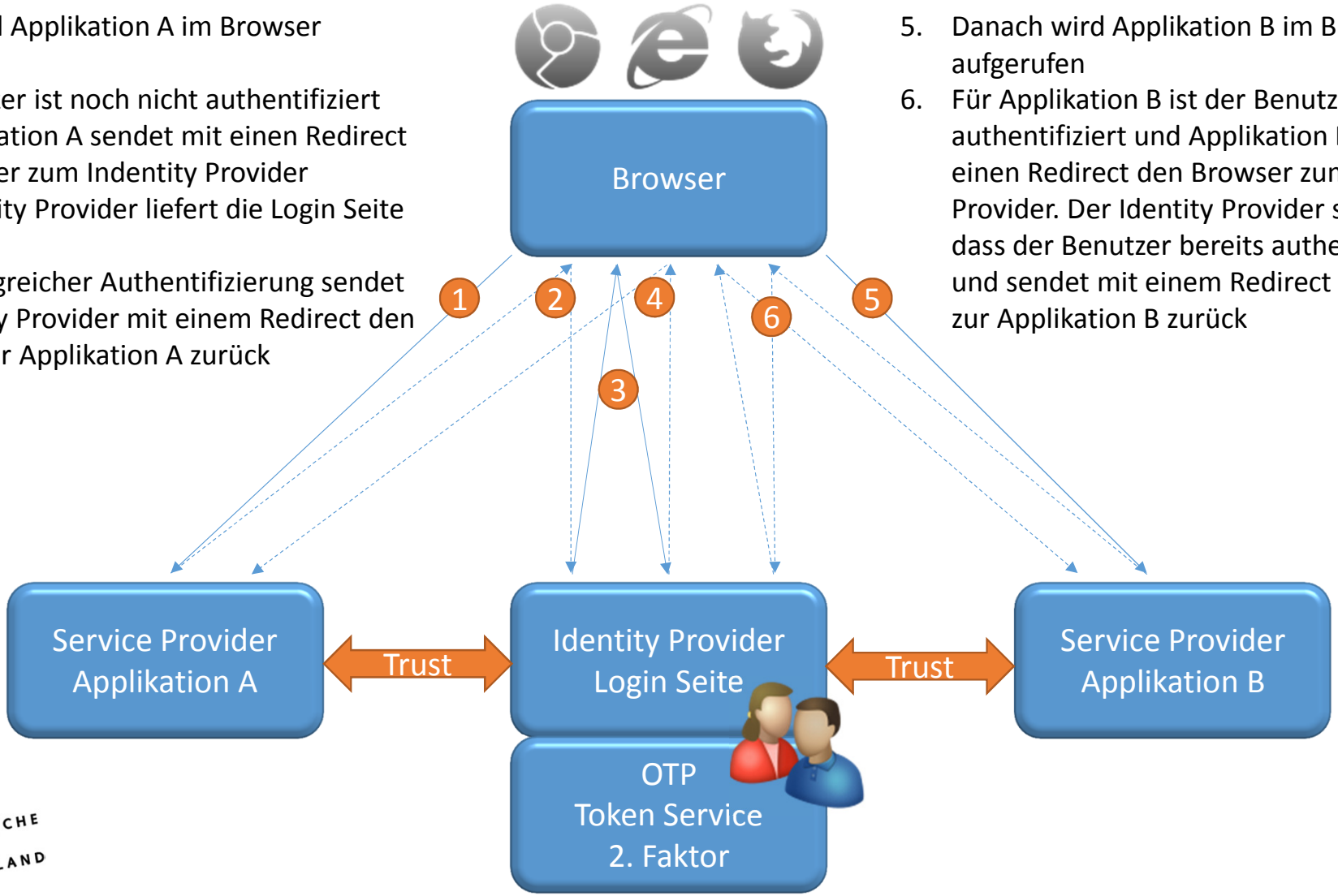
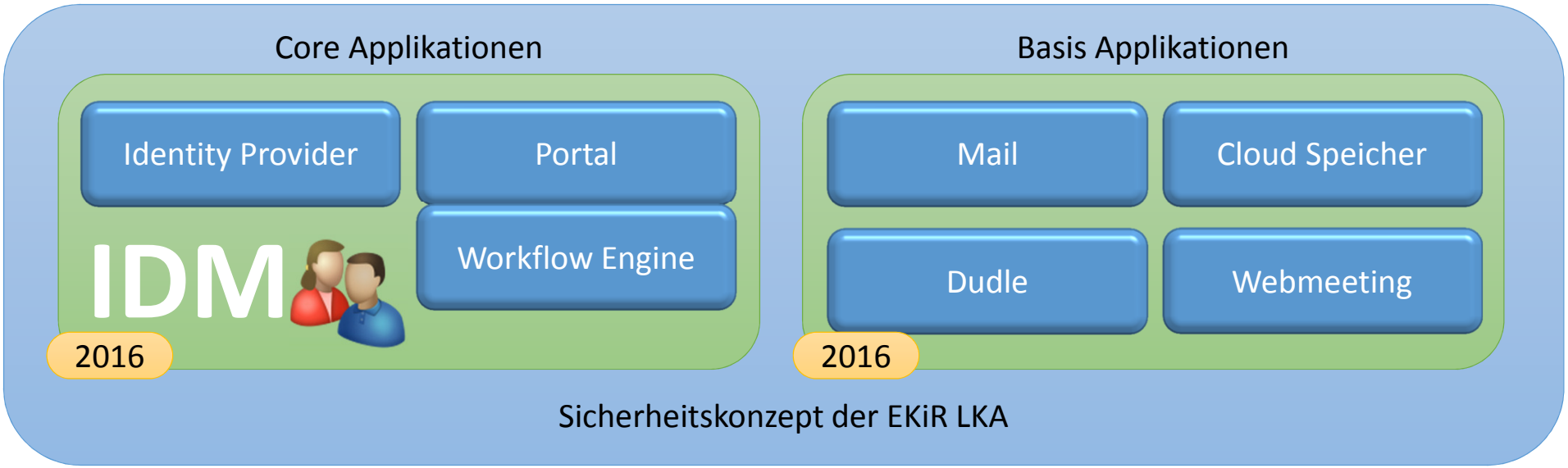
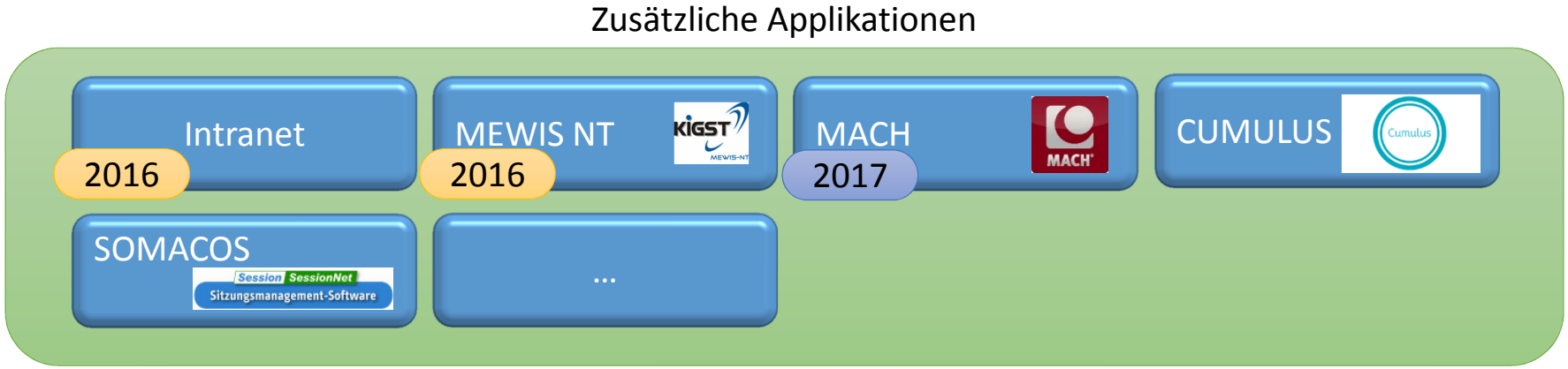
1. Zuerst wird Applikation A im Browser aufgerufen
2. Der Benutzer ist noch nicht authentifiziert und Applikation A sendet mit einen Redirect den Browser zum Indentity Provider
3. Der Indentity Provider liefert die Login Seite aus
4. Nach erfolgreicher Authentifizierung sendet der Identity Provider mit einem Redirect den Browser zur Applikation A zurück



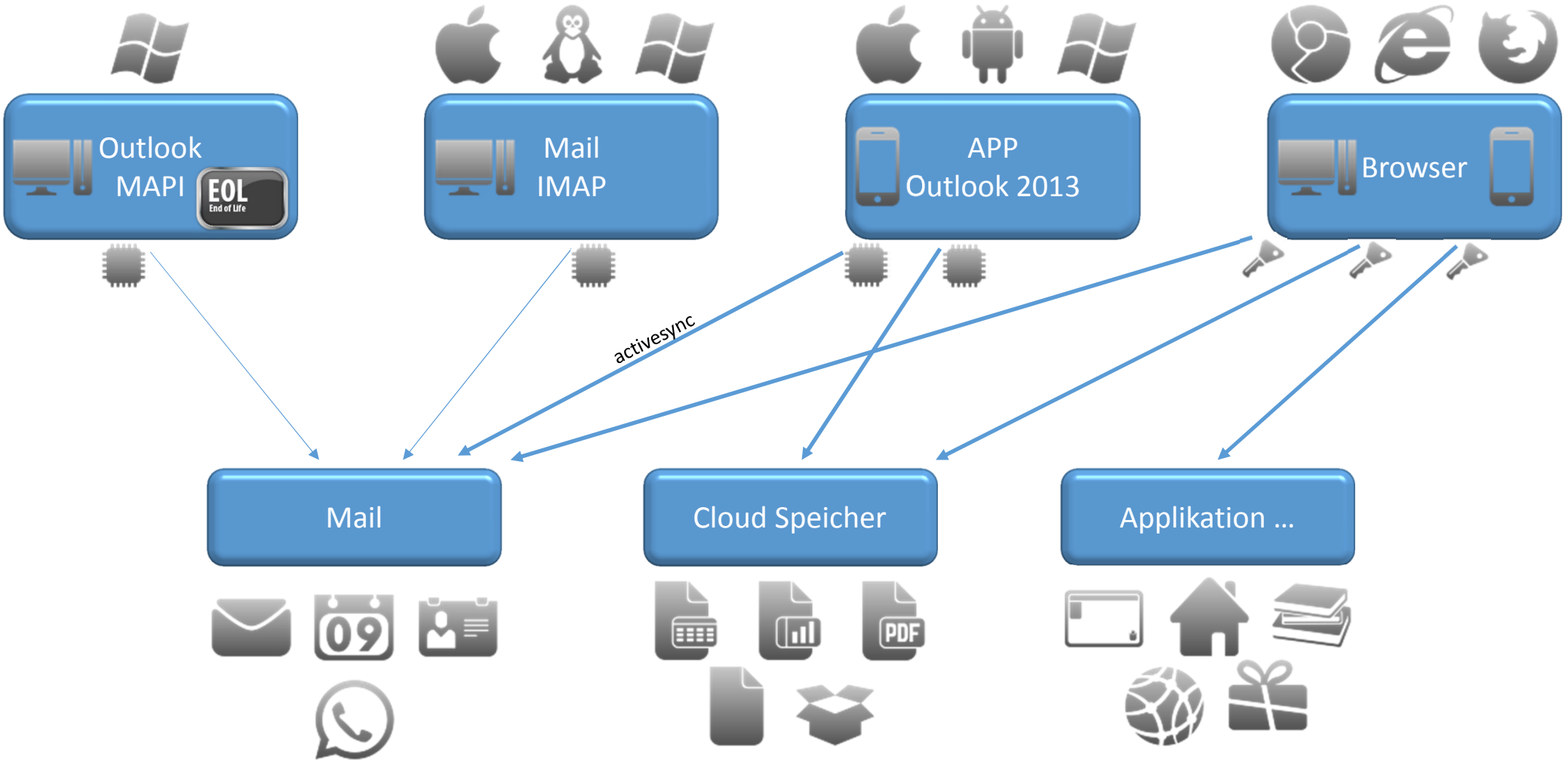
5. Danach wird Applikation B im Browser aufgerufen
6. Für Applikation B ist der Benutzer noch nicht authentifiziert und Applikation B sendet mit einen Redirect den Browser zum Indentity Provider. Der Identity Provider stellt fest, dass der Benutzer bereits authentifiziert ist und sendet mit einem Redirect den Browser zur Applikation B zurück

EVANGELISCHE KIRCHE IM RHEINLAND





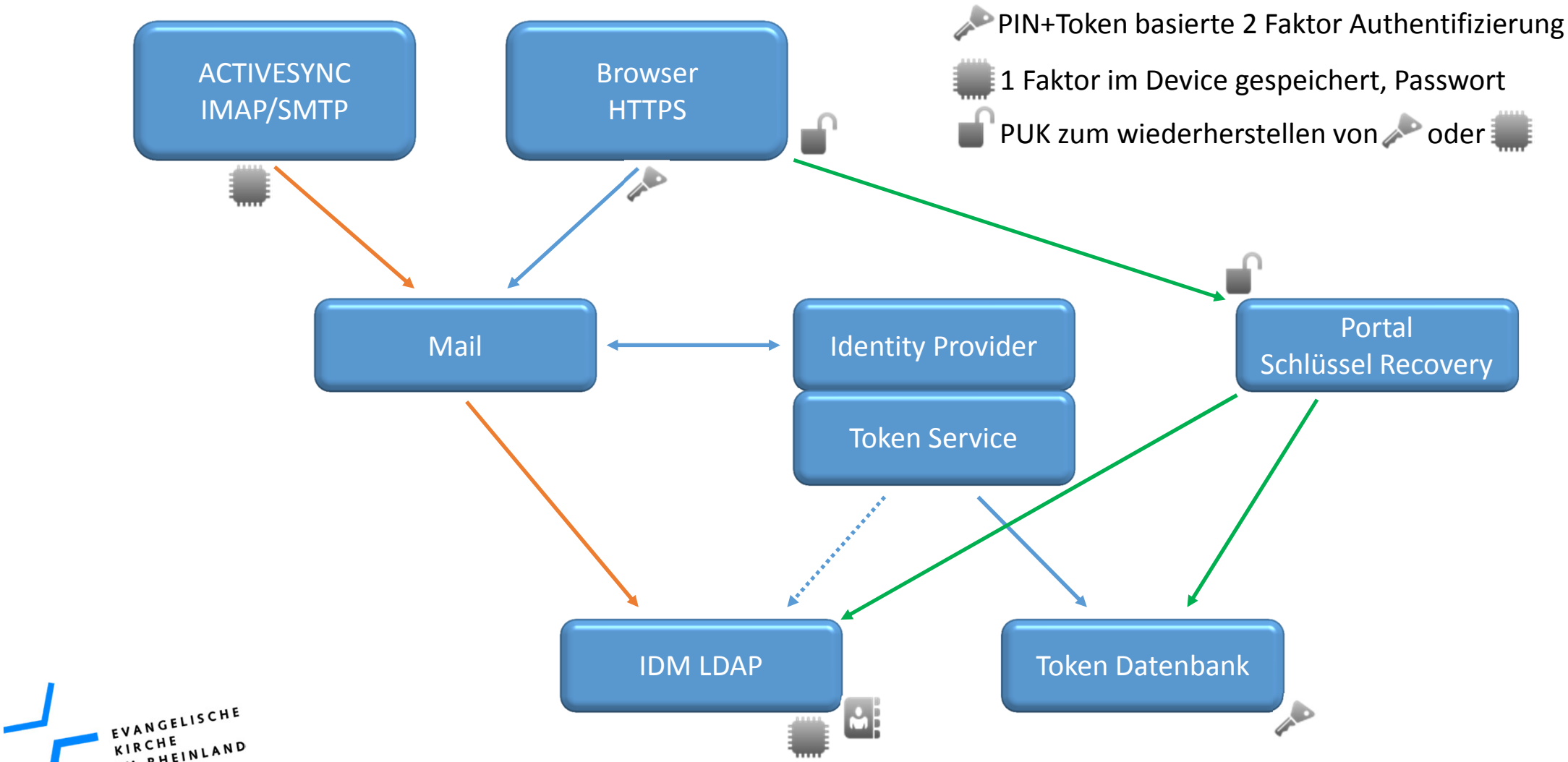
EVANGELISCHE KIRCHE IM RHEINLAND



EVANGELISCHE KIRCHE IM RHEINLAND

PIN+Token basierte 2 Faktor Authentifizierung

1 Faktor im Device gespeichert, Passwort



EVANGELISCHE KIRCHE IM RHEINLAND