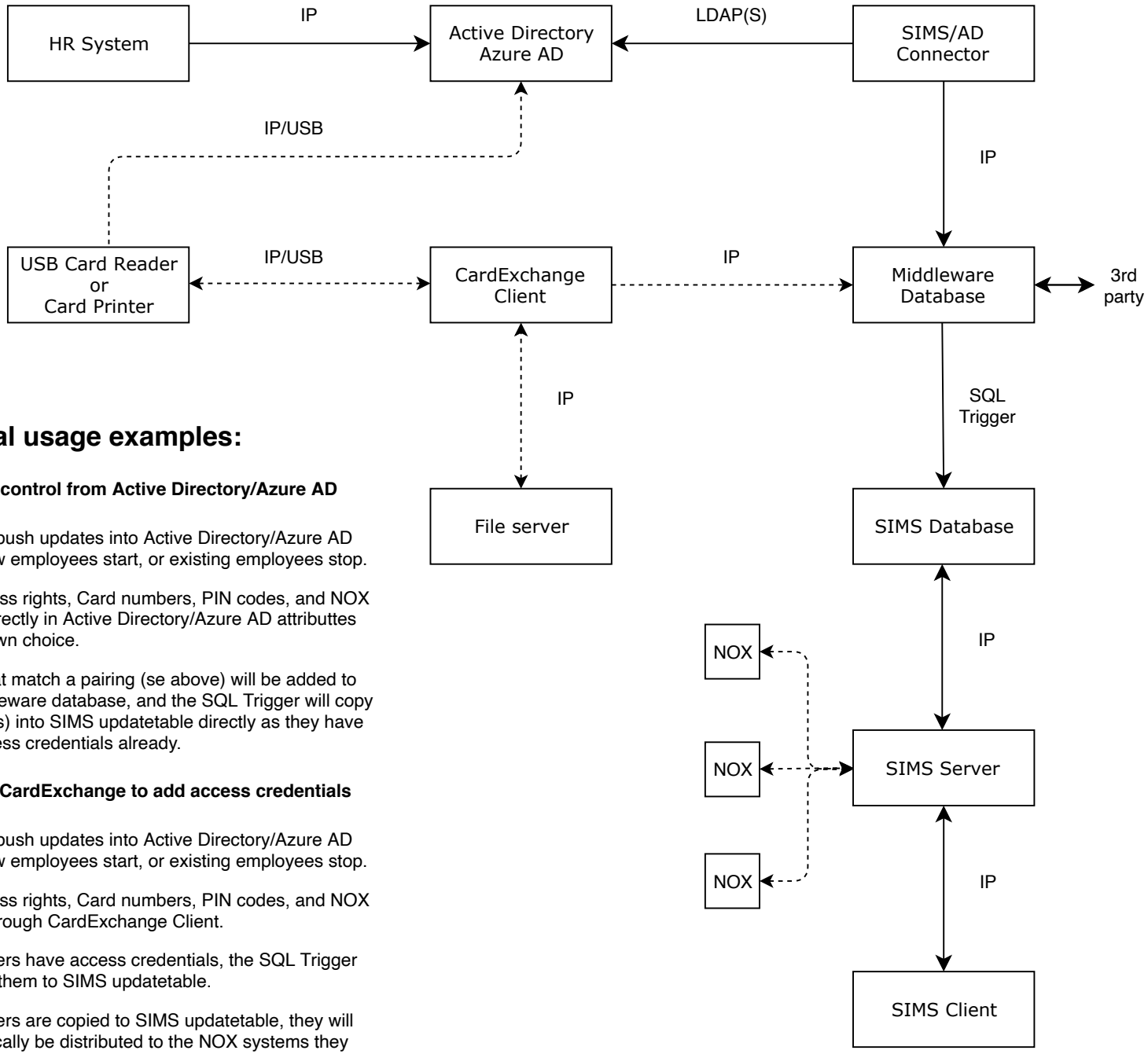
SIMS Active Directory and Azure AD integration



How does it work?

The integration works in multiple way, depending on how the owner wants to handle the user creation, and access rights management.

Common feature is that the SIMS/AD Connector scans for changes by a predefined interval from 1 minute and up. Typical is either once per hour or once per day. It is possible to run the synchronisation on demand when needed.

Users in SIMS will be constructed by using First name, Last name and SamAccountName to keep users unique.

Controling users from Active Directory/Azure AD supports the following attributes:

- Creation of users
- Deletion of users
- Disabling of users
- Expiration date on users
- Global Security Group pairing with SIMS Profiles
- Global Security Group pairing with SIMS Area Groups
- OU pairing with SIMS Profiles
- OU pairing with SIMS Area Groups
- Contacts created in Active Directory can also be paired same as users
- Nested Groups

Typical usage examples:

1. Direct control from Active Directory/Azure AD

HR data push updates into Active Directory/Azure AD when new employees start, or existing employees stop.

Add access rights, Card numbers, PIN codes, and NOX Codes directly in Active Directory/Azure AD attributtes of your own choice.

Users that match a pairing (se above) will be added to the middleware database, and the SQL Trigger will copy the user(s) into SIMS updatetable directly as they have their access credentials already.

2. Using CardExchange to add access credentials

HR data push updates into Active Directory/Azure AD when new employees start, or existing employees stop.

Add access rights, Card numbers, PIN codes, and NOX Codes through CardExchange Client.

When users have access credentials, the SQL Trigger will copy them to SIMS updatetable.

When users are copied to SIMS updatetable, they will automatically be distributed to the NOX systems they are given access to in their SIMS Profile, or SIMS Area Group.