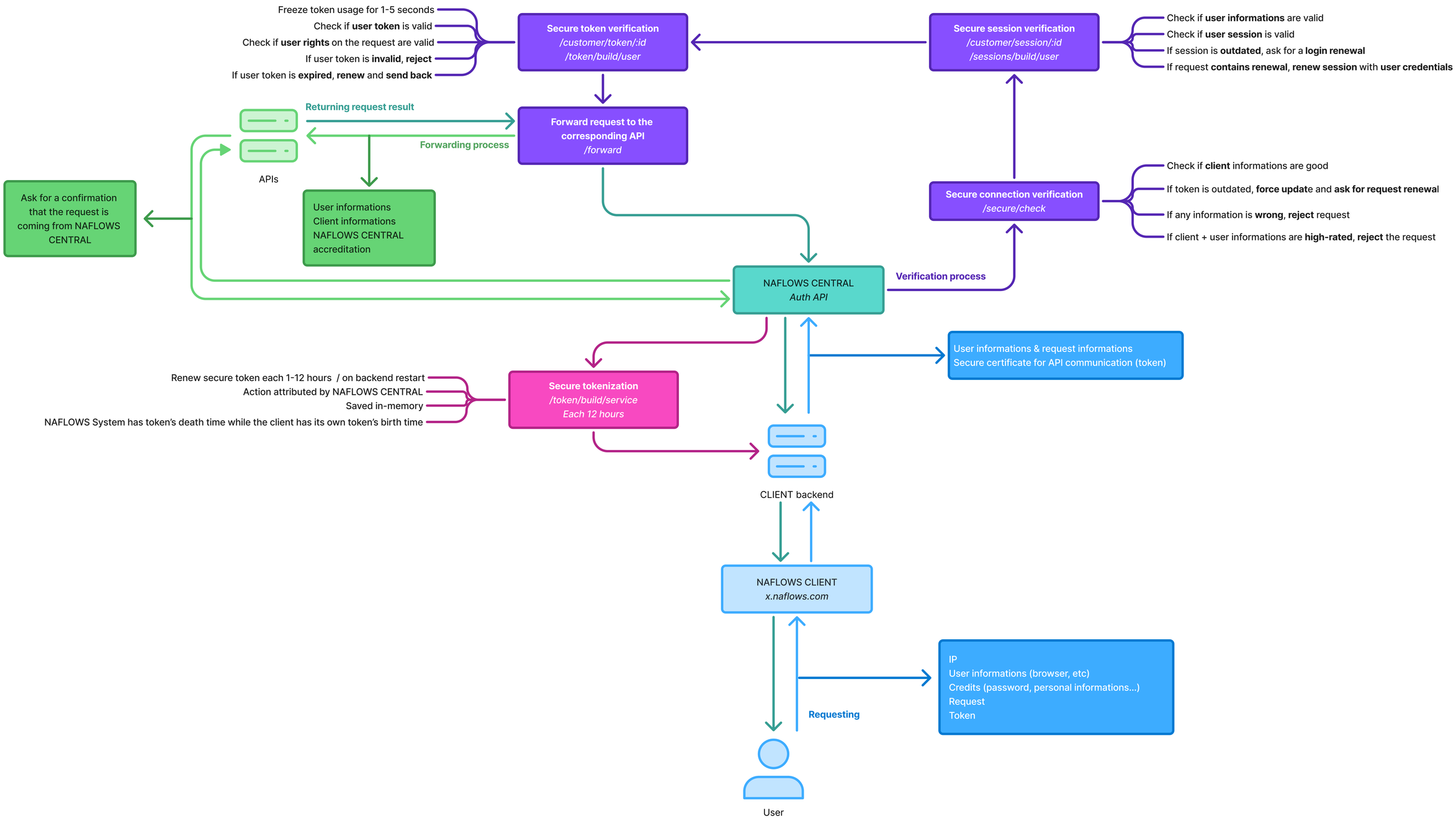
Freeze token usage for 1-5 seconds
Check if user token is valid
Check if user rights on the request are valid
If user token is invalid, reject
If user token is expired, renew and send back
Secure token verification
/customer/token/:id
/token/build/user
Secure session verification
/customer/session/:id
/sessions/build/user
Check if user informations are valid
Check if user session is valid
If session is outdated, ask for a login renewal
If request contains renewal, renew session with user credentials
Returning request result
Forwarding process
APIs
Forward request to the corresponding API
/forward
Ask for a confirmation that the request is coming from NAFLOWS CENTRAL
User informations
Client informations
NAFLOWS CENTRAL accreditation
Secure connection verification
/secure/check
Check if client informations are good
If token is outdated, force update and ask for request renewal
If any information is wrong, reject request
If client + user informations are high-rated, reject the request
NAFLOWS CENTRAL
Auth API
Verification process
User informations & request informations
Secure certificate for API communication (token)
Renew secure token each 1-12 hours / on backend restart
Action attributed by NAFLOWS CENTRAL
Saved in-memory
NAFLOWS System has token's death time while the client has its own token's birth time
Secure tokenization
/token/build/service
Each 12 hours
CLIENT backend
NAFLOWS CLIENT
x.naflows.com
IP
User informations (browser, etc)
Credits (password, personal informations...)
Request
Token
Requesting
User