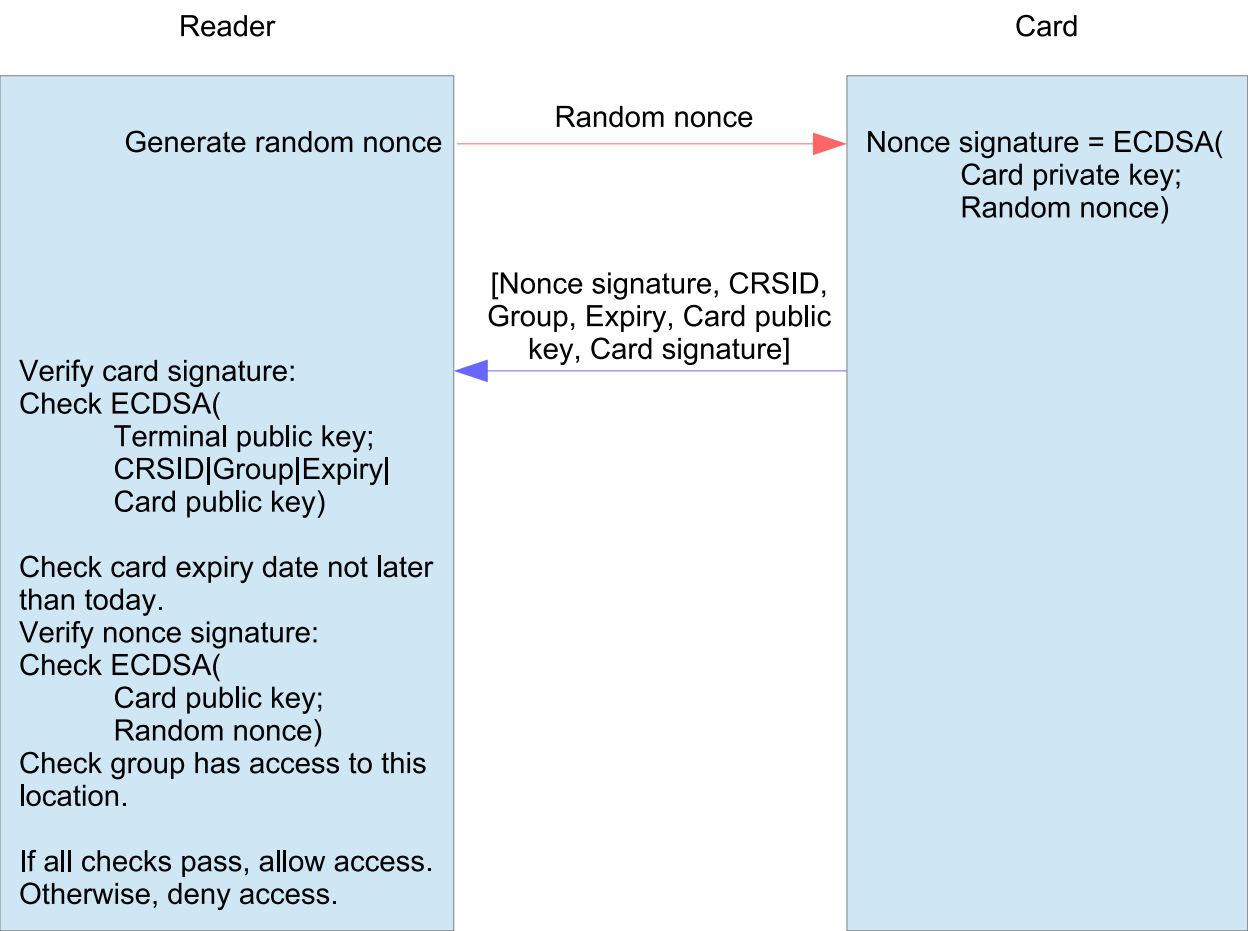
Reader
Card
Generate random nonce
Random nonce
Nonce signature = ECDSA(
Card private key;
Random nonce)
[Nonce signature, CRSID, Group, Expiry, Card public key, Card signature]
Verify card signature:
Check ECDSA(
Terminal public key;
CRSID|Group|Expiry|
Card public key)
Check card expiry date not later than today.
Verify nonce signature:
Check ECDSA(
Card public key;
Random nonce)
Check group has access to this location.
If all checks pass, allow access. Otherwise, deny access.