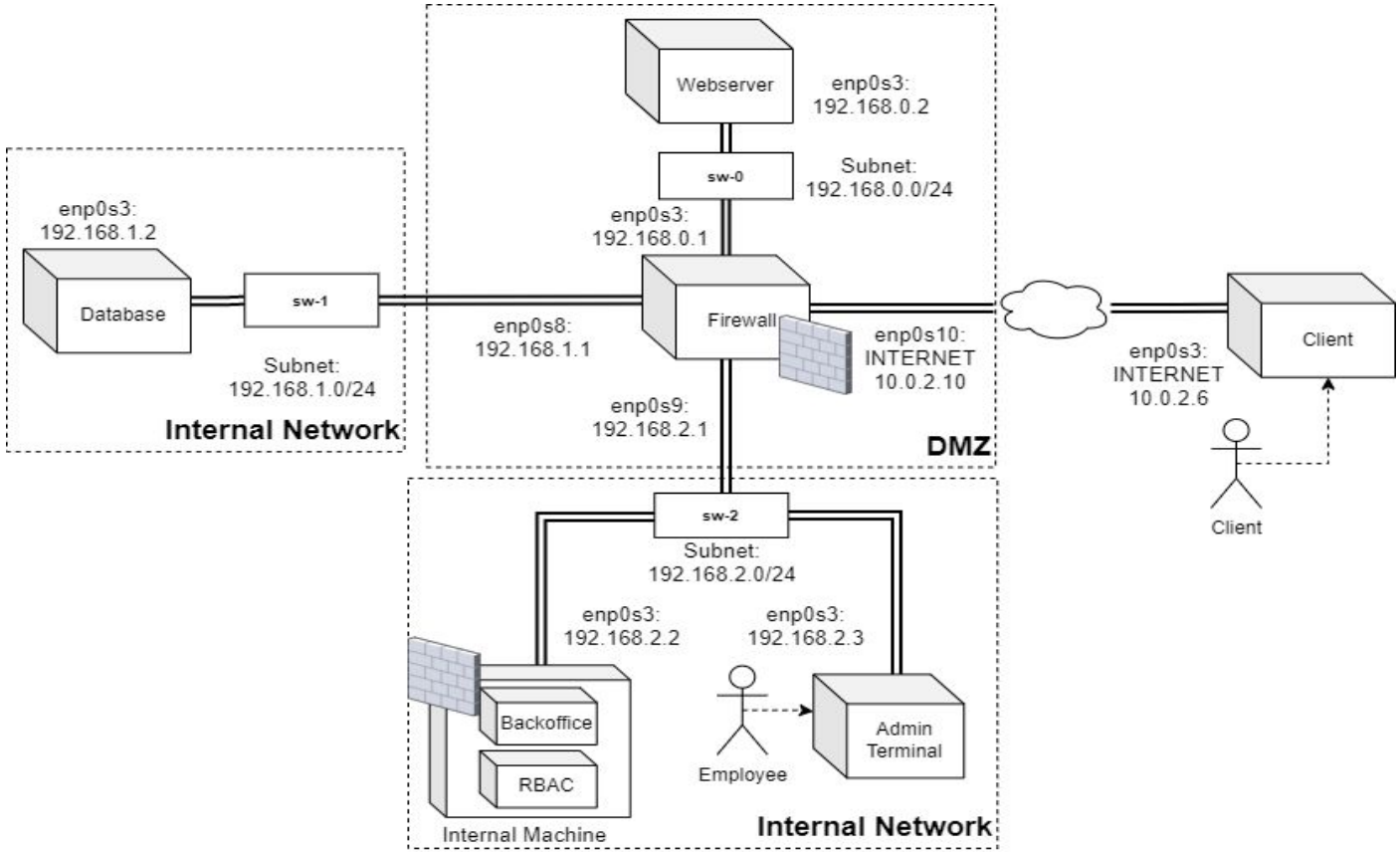
TÉCNICO LISBOA

EcoGes

Network and Computer Security
Alameda

Group 41
92475 Henrique Cavaco
92513 Mafalda Ferreira
105458 João Moreira

Infrastructure



Secure Channels

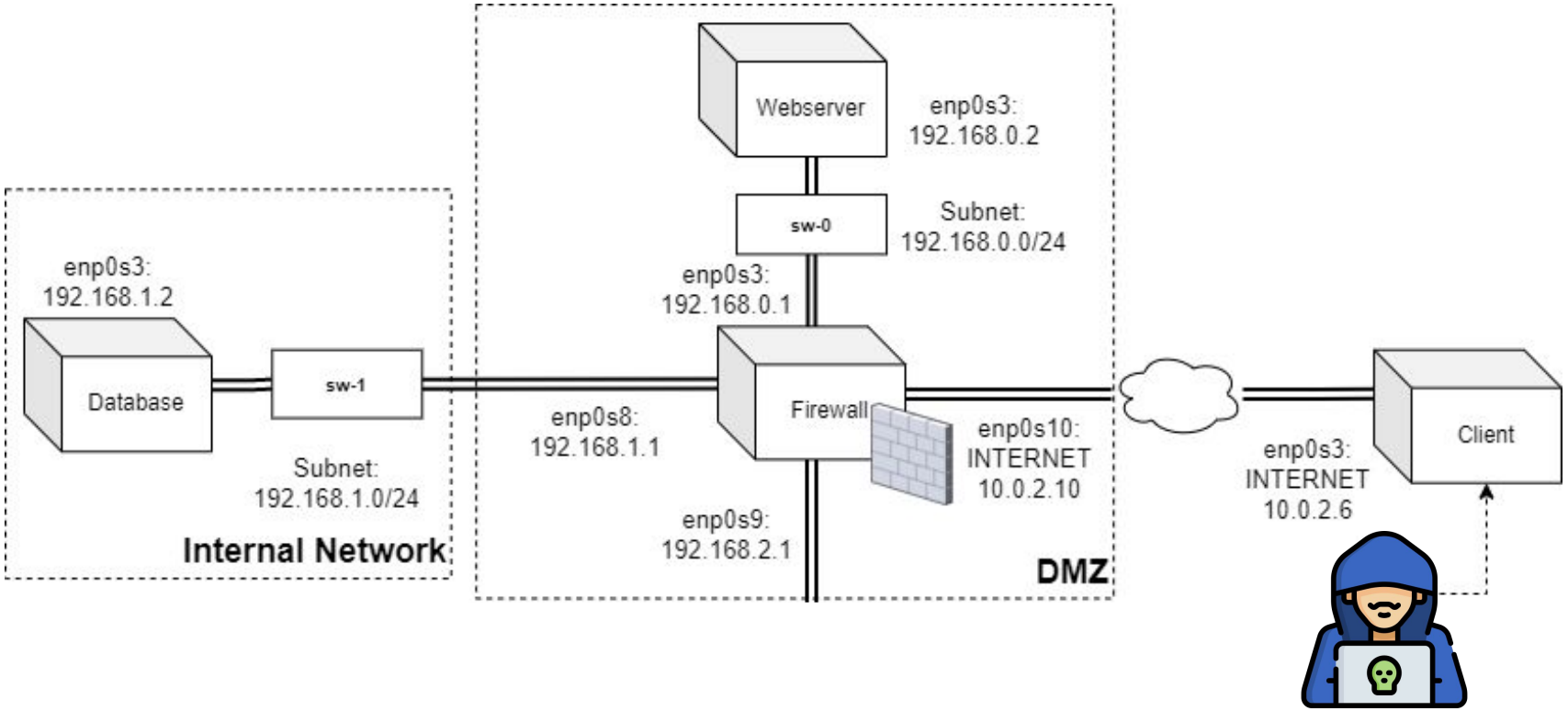
- One-way TLS
- Local CA that signs all certificates
- Servers have their certificate and private key in a keystore
- Clients have the server's and CA's certificates in a truststore
- Clients validate the server's certificate chain with the CA's certificate

(client)	→	(server)
client	→	webserver
admin	→	backoffice
webserver	→	database
backoffice	→	database
backoffice	→	RBAC
backoffice	→	webserver

Security Challenge - Introduction

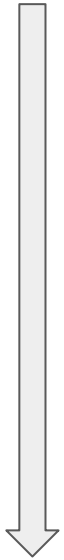
- Assume client's credentials can be stolen
- Energy management employees cannot access user's personal data
- Account management employees cannot access user's energy management data

Security Challenge - Data Obfuscation



Security Challenge - Data Obfuscation

IBAN: 484201298729348299372



IBAN: **********372

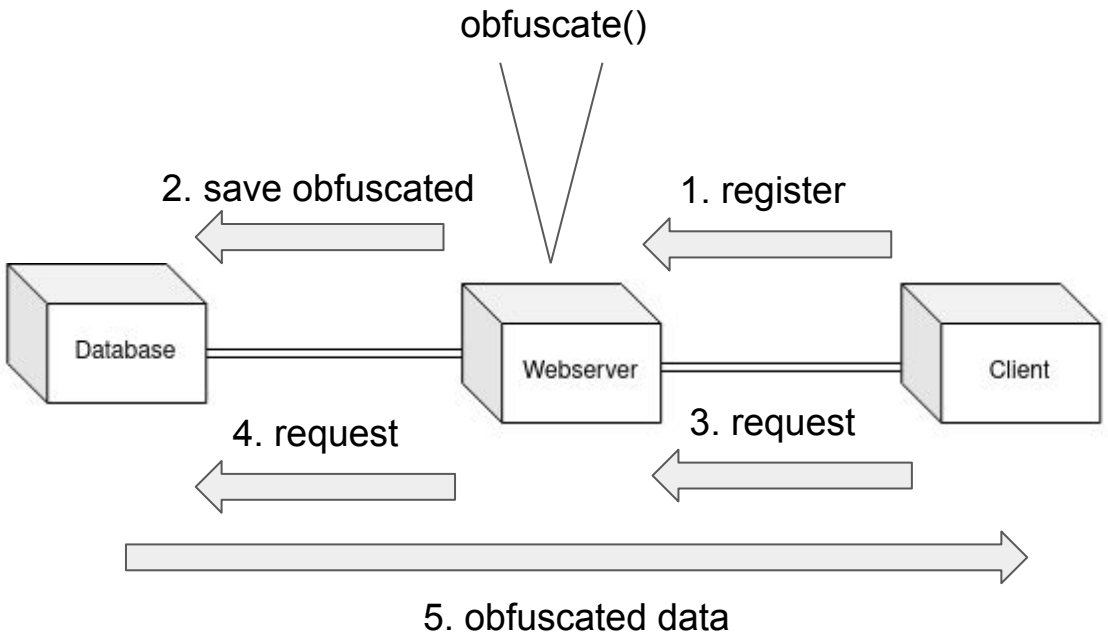
```
private String obfuscate(String text){
    int len = text.length();
    if (text == null || len <= 1) {
        return "***";
    }
    char[] chars = text.toCharArray();

    if (len == 2){
        chars[0] = '*';
        return new String(chars);
    } else if (len == 3){
        chars[0] = '*';
        chars[1] = '*';
        return new String(chars);
    } else if (len == 4){
        chars[0] = '*';
        chars[1] = '*';
        chars[2] = '*';
        return new String(chars);
    }

    for (int i = 0; i < chars.length - 3; i++) {
        chars[i] = '*';
    }
    return new String(chars);
}
```

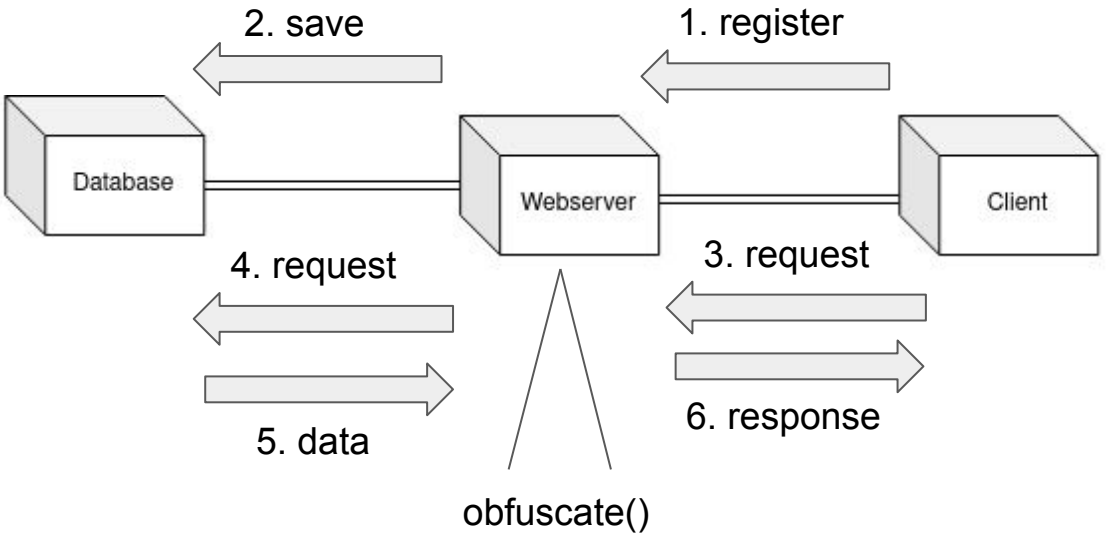
Security Challenge - Data Obfuscation

Energy consumption/production Data

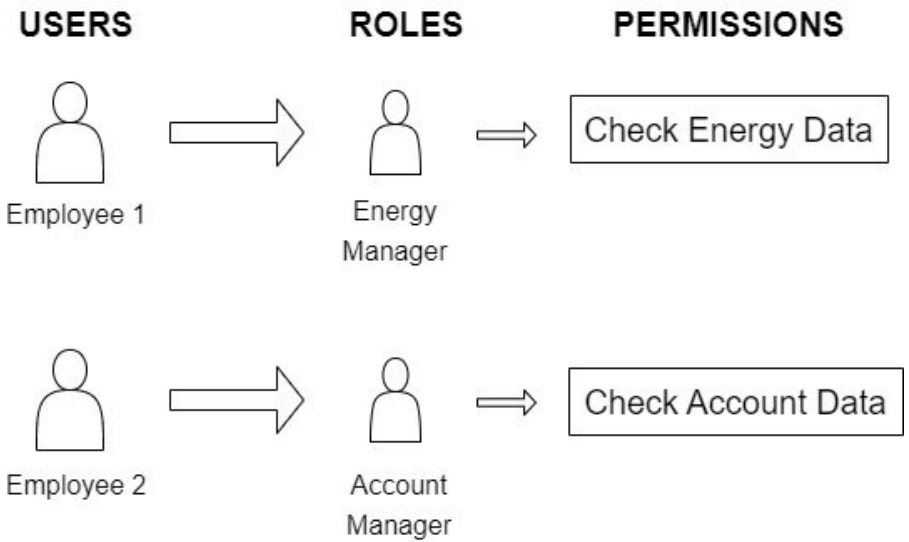


Security Challenge - Data Obfuscation

Personal Data



Security Challenge - Access Control (1/2)
Role-**B**ased **A**ccess **C**ontrol (**RBAC**) mechanism

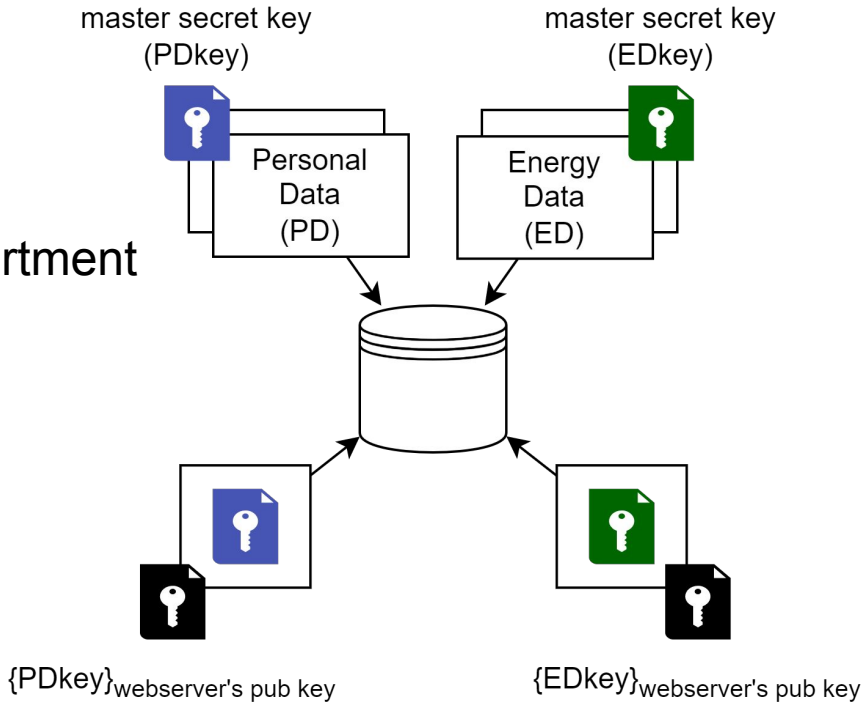


Security Challenge - Access Control (2/2)

1. **Admin** requests data to **backoffice**
2. **Backoffice** asks authorization (request) to **RBAC**
3. **RBAC** grants authorization (response) by generating a **Ticket** and it's signature
4. Explained further ahead

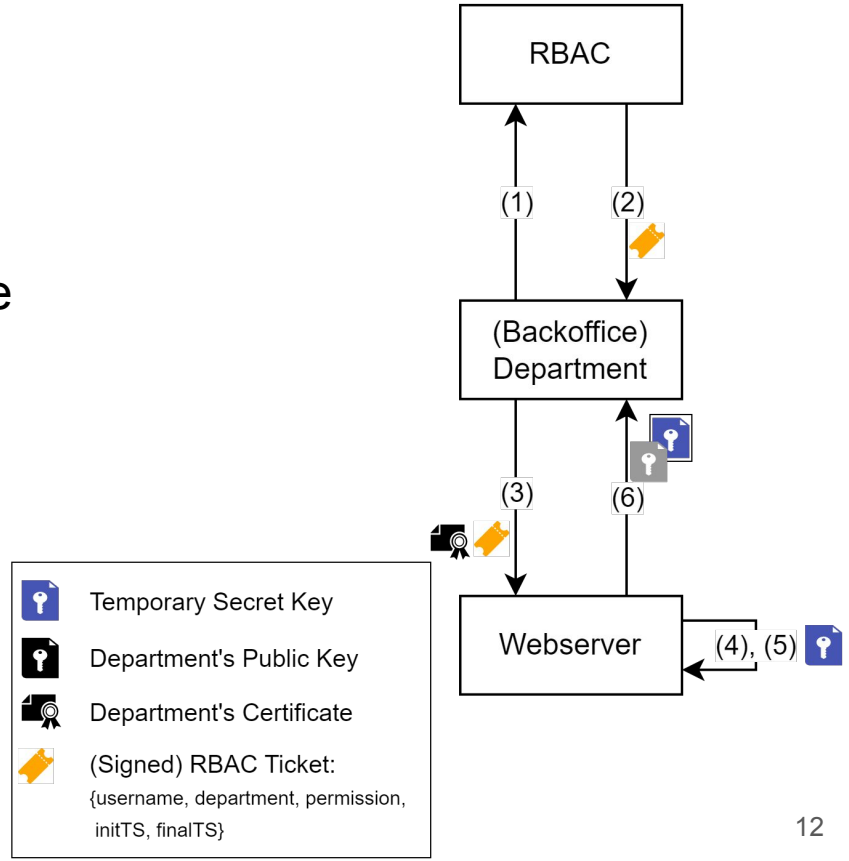
Security Challenge - Data Separation

- Webserver manages data separation with encryption
- One master secret key per data compartment
  - AES encryption using CBC mode
- **Confidentiality** of master secret keys



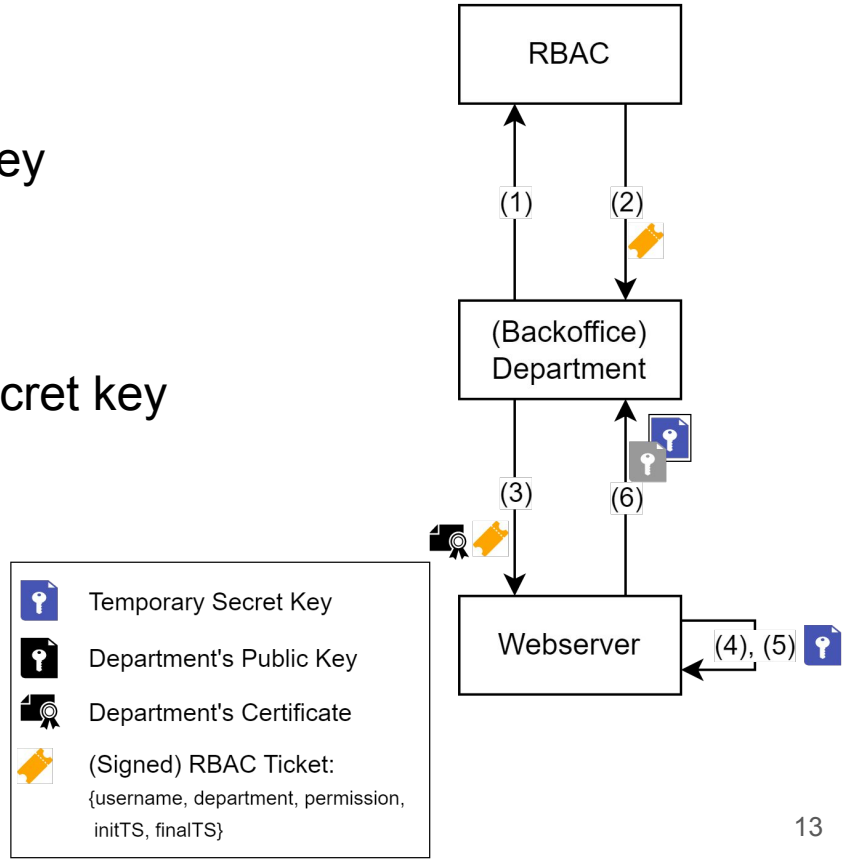
Security Challenge - Data Separation Sharing Keys (1/2)

1. Department requests access to RBAC
2. RBAC responds with Ticket and signature
3. Department requests secret keys
   - RBAC ticket & RBAC signature
   - Department's certificate & request signature
   - **Authenticity & integrity**
4. Webserver validates request



Security Challenge - Data Separation Sharing Keys (2/2)

5. Webserver generates temporary secret key
   - One-time use key
   - Re-encryption of data
6. Webserver shares wrapped temporary secret key
   - **Confidentiality**
7. Department unwraps temporary secret key and decrypts client's data



Conclusion

- With the accomplishment of this project, we realized it is not possible to achieve perfect security

- Although, we believe our solution effectively protects the access to client data with compartmentalization through the usage of encryption (**main objective**)