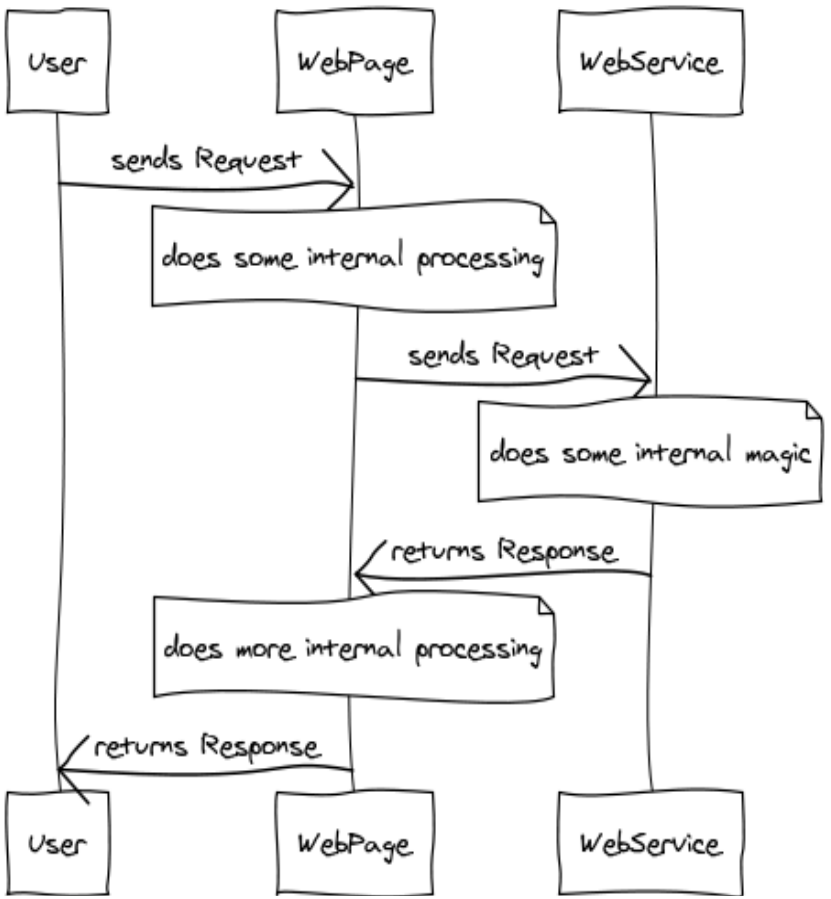
UON.Zerberuss

Content

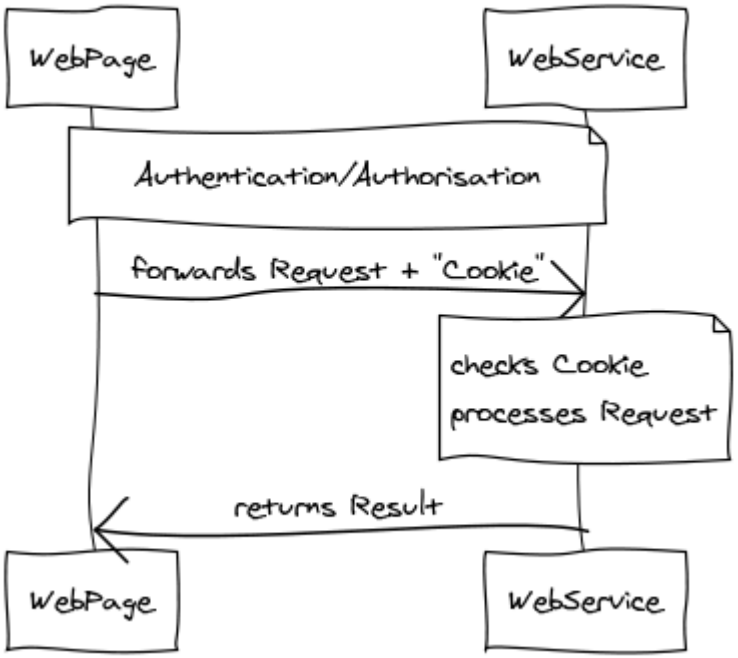
Use Cases



Examples:

1. User Authentication
2. Mass Mailer
3. eCommerce
4. Payment
5. Publishing
6. ….

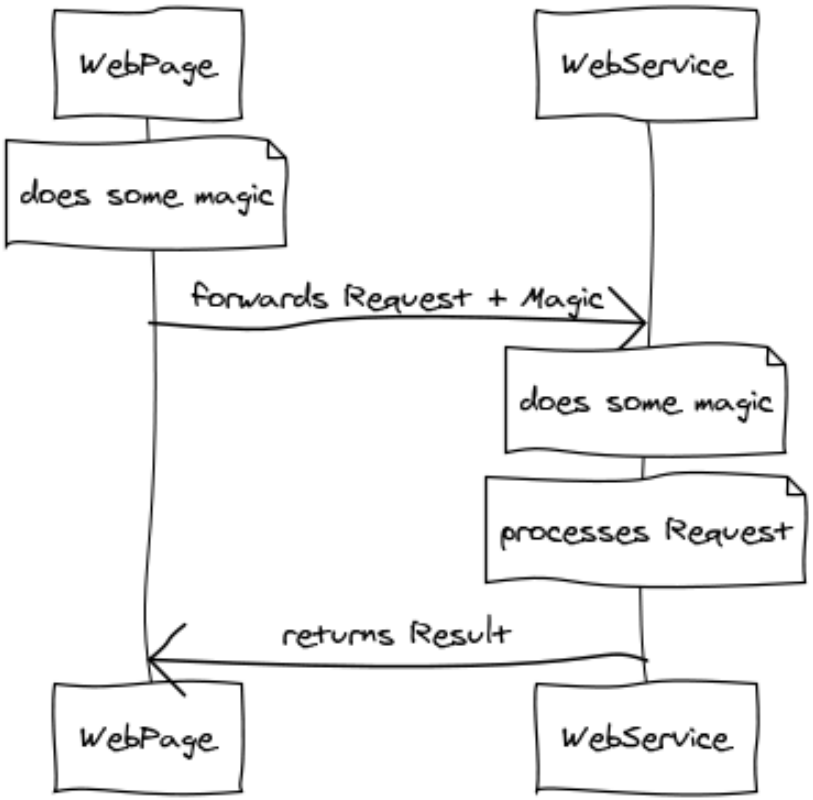
Communication Details



Cons:

1. one Request for A²
2. WebService NOT stateless
3. Request easy to manipulate
   - ➲ Solution: SSL, but expensive
4. Keep alive required
5. Not protection against replay

Targeted Communication



Pros:

1. one Request to
   - authenticate source
   - protect data
   - limit replay risk

?

GNU Privacy Guard (GPG)

1. Full replacement of PGP
2. Does not use any patented algorithms
3. GPLed, written from scratch
4. Maintained
5. Supports
   - ElGamal, DSA, RSA, AES, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 and TIGER
   - easy implementation of new algorithms using extension module
6. Supports key and signature expiration date
7. Integrated support for HKP keyservers

How does GPG helps?

1. Timestamp in signature
   - ➲ limits replay attacks
2. Can use all forwarded attributes for signature
   - ➲ secures transferred data
3. Javascript to encrypted data
   - ➲ protects confidential data with public key of WebService

FLOW3 ACL policy

Pros:

1. controlls access to
   - Controllers
   - Methods

Cons:

1. always sets cookies
   - NOT stateless
2. throws exception
   - difficult to handle in S²-communication

GPG Requirements

1. php-pear (Ubuntu)
2. libgpgme11-dev (Ubuntu)
3. pecl install gnupgp
4. Add gnupg.so to php.ini if not done automatically

Tasks

1. Make FLOW3 cookie setting configurable
2. Extend FLOW3 error handling of wrong authentication
3. Implement GPG-Authentication:
   - Security\Cryptography\GPGWalletServiceInterface
   - Security\Cryptography\GPGWalletService
   - Security\AccountFactory

FLOW3 Auto Cookie

AuthenticationProviderManager::authenticate

```
129         * @throws \TYPO3\FLOW3\Security\Exception\Authenticatior
130         * @FLOW3\Session(autoStart=true)
131         */
132        public function authenticate() {
133                $anyTokenAuthenticated = FALSE;
134                if ($this->securityContext === NULL) throw new \T
135
136                $tokens = $this->securityContext->getAuthenticati
137                if (count($tokens) === 0) {
138                        throw new \TYPO3\FLOW3\Security\Exceptior
139                }
```

FLOW3 Session Handling

Package::boot

```
44                $dispatcher->connect('TYPO3\FLOW3\Command\CoreCommandControll
45
46                $dispatcher->connect('TYPO3\FLOW3\Security\Authentication\Aut
47                $dispatcher->connect('TYPO3\FLOW3\Security\Authentication\Aut
48            }
```

Links

1. http://forge.typo3.org/projects/package-zerberuss
2. https://svn.typo3.org/FLOW3/Packages/Zerberuss
3. Twitter #uon_li